Contents

COMPUTER NETWORKS (VI-SEM)

UNIT-I : INTRODUCTION PAGE N

Computer Network – Definitions, goals, components, Architecture, Classifications & Types ..... (03 to 1

Layered Architecture – Protocol hierarchy, Design issues, Interfaces and Services, Connection-oriented & Connectionless Services, Service primitives, Design issues & its functionality ..... (17 to 2

ISO-OSI Reference Model – Principle, Model, Descriptions of various layers and its comparison with TCP/IP ..... (26 to 3

Principles of physical layer – Media, Bandwidth, Data rate and Modulations ..... (36 to 5

UNIT-II : DATA LINK LAYER

Data Link Layer – Need, Services Provided, Framing, Flow Control, Error Control ..... (55 to 6

Data Link Layer Protocol – Elementary & Sliding Window Protocol – 1-bit, Go-Back-N, Selective Repeat, Hybrid ARQ ..... (63 to 8

Protocol verification – Finite State Machine Models & Petri net models .... (87 to 9

ARP/RARP/GARP ..... (91 to 9

UNIT-III : MAC SUBLAYER

MAC Sublayer – MAC Addressing, Binary Exponential Back-off (BEB) Algorithm ..... (97 to 10

Distributed Random Access Schemes/Contention Schemes – For Data Services (ALOHA and Slotted-ALOHA), for Local-Area Networks (CSMA, CSMA/CD, CSMA/CA) ..... (102 to 12

Collision Free Protocols – Basic Bit Map, BRAP, Binary Count Down, MLMA, Limited Contention Protocols – Adaptive Tree Walk ..... (121 to 12

Performance Measuring Metrics, IEEE Standards 802 series & their variant ..... (128 to 14

UNIT-IV : NETWORK LAYER

Network Layer – Need, Services Provided, Design issues, Routing Algorithms – Least Cost Routing Algorithm, Dijkstra's Algorithm, Bellman-Ford Algorithm, Hierarchical Routing, Broadcast Routing, Multicast Routing ..... (143 to 16

IP Addresses, Header format, Packet forwarding, Fragmentation and reassembly, ICMP, Comparative study of IPv4 & IPv6 ..... (165 to 18

UNIT-V : TRANSPORT AND APPLICATION LAYERS

Transport Layer – Design Issues, UDP – Header Format, Per-segment Checksum, Carrying Unicast/Multicast Real-time Traffic ..... (183 to 18

TCP – Connection Management, Reliability of Data transfers, TCP Flow Control, TCP congestion Control, TCP Header Format, TCP Timer Management ..... (189 to 20

Application Layer – WWW and HTTP, FTP, SSH, Email (SMTP, MIME, IMAP), DNS, Network Management (SNMP) ..... (204 to 22

UNIT 1

INTRODUCTION

COMPUTER NETWORK – DEFINITIONS, GOALS, COMPONENTS, ARCHITECTURE, CLASSIFICATIONS & TYPES

Q.1. What is computer network ? Write advantages of computer network. ***(R.G.P.V., June 2013)***

Ans. The term ***"computer network"*** refers to an interconnected collection of autonomous computers. When two computers are able to exchange information, then they are said to be interconnected. The connection require not be through a copper wire; lasers, microwaves and communication satellites can also be used. By requiring the computers to be ***autonomous*** we wish to exclude from our definition systems in which there is a clear master/slave relation. The computers are not autonomous when one computer can forcibly start, stop or control another one. A system with one control unit and many slaves is neither a network nor a large computer with remote card readers, printers and terminals.

Advantages of computer network are as follows –

(i) Faster Data Transfer – A network provides the means to exchange data among computers and to make programs and data available to the people.

(ii) Resource Sharing – It permits the sharing of resources of the machines with the goal to make data available to everyone without regard to the physical location of the resource and the user.

(iii) Distributed Processing – Networking provides the facility of distributed processing among the multiple autonomous computers.

(iv) Higher Reliability and Accuracy – One of the aim of networking is to provide reliability by having alternative source of supply. Networking also provides the critical function of back-up.

Q.2. What is computer network and how it is different from distributed system ? ***(R.G.P.V., Dec. 2012)***

Ans. **Computer Network** – Refer the ans. of Q.1.

There is a considerable difference between a distributed system and computer network. The key distinction is that in a distributed system, the existence of multiple autonomous computers is transparent (i.e., not visible to the user. Here, nothing has to be done explicitly; it is all automatically done by the system without the users knowledge. With a network a user must explicitly log onto one machine, explicitly submit jobs remotely, explicitly move files around and generally handle all the network management personally.

In effect, a distributed system is a special case of a network, one whose software gives it a high degree of cohesiveness and transparency. Thus the distinction between a network and a distributed system lies with the software (especially the operating system), rather than with the hardware.

Q.3. Write the goals of computer networking with its classification.
(R.G.P.V., May 20

Ans. The most important goals of computer networks are –

(i) Reliability Goals – Network reliability can be measured by the networks robustness in a catastrophe, failure frequency and average down time of network. These are described as follows –

(a) Catastrophe – Network should be protected from catastrophe events like theft or earthquake. One protection of network against these is a reliable system to backup network software.

(b) Failure Frequency – A network which fails rarely is good for a user but a network which fails oftently is of little value to a user.

(c) Average Down Time – How long does it take to restore service is called down time. A network with less value of average down time is more important than one that does not.

(ii) Performance Goals – The network performance is measured with its transit time and response time. Transit time is the time needed for message to travel from one device to another device in network. Response time is the amount of time elapsed between an inquiry and a response. Network performance depends on a number of factors, which are given below –

(a) Software – Travelling a message from node to node through a network needs processing for transformation of raw data into transmittable signals, to ensure error free delivery to route these signals to the proper destination and to recast the signals into a farm the receiver can use. The software which gives these type of services affects both the speed and the reliability of a network link. Well-designed software can speed the process and provide transmission more efficient and effective.

(b) Hardware – Both the speed and capacity of transmission are affected by the types of hardware. A higher speed system with greater storage capacity gives better performance.

(c) Network Transmission Medium – A network transmission medium may be wireless (microwave, satellite, etc.) or wired (optical fiber, copper cables, etc.). The transmission medium defines the data rate (speed at which data can move through a connection). Faster and faster transmission media is needed for networks as the uses of network are increasing, like fiber optic cabling. Amount of data that a transmission media can control defines its capacity and in turn how powerful media it is.

(d) Traffic Load – The network design is dependent on an assessment of the average number of users that will be communicating at any moment of time. Having a large number of concurrent users may slow response time in a network not designed to coordinate heavy traffic loads. In peak load periods however the "actual number of users" can exceed the average "number of users" and thereby deteriorate the performance.

(iii) Security Goals – Network security issues comprise of protecting data from unauthorized access and prevention from virus attacks.

(a) Unauthorized Access – Protection of sensitive data from unauthorized access is mandatory for any network to be useful. Protection can be done at a number of levels. At the high level are encryption methods. At lowest level are user login codes and passwords.

(b) Viruses – Since a network is accessible from many points, it can be susceptible to computer viruses. A virus is an illicitly introduced code to damage the functionality of a system. A good network is protected from viruses by hardware and software designed specifically for that purposes.

(iv) Network Cost – The network cost is calculated on the following –

(a) Runtime Cost – To control a network functionally strong, very good maintenance is needed and as much complexity we increase in design chances of failure increases accordingly which in turn leads to more down time and maintenance cost of network.

(b) Fixed Cost – The cost of transmission medium and devices (such as router, switch, hub, etc.) which are needed to make a network functional plays an important role while designing the network. For better network design in minimum cost the network design engineer should understand the function's to be performed by the network and accordingly performance parameters of medium and device (capacity and quality of medium, processing speed, capacity, etc., of device) must be selected.

So while designing not only fixed cost but run-time costs should be considered into account for minimization of total cost.

Q.4. What are the applications of computer network ?

Or

What are the uses of computer network now-a-days ?

(R.G.P.V., June 201

Ans. Some of the network applications in different fields are the following:

(i) Marketing and Sales – Computer networks are widely used i both marketing and sales firms. These are used by the marketing professiona to collect, exchange, and analyzes data relating to customer requirements an product development cycles. Teleshopping is also an important part of sale applications, that uses order-entry computers or telephones connected to a order-processing networks, and on-line reservation services for hotels airline and so on.

(ii) Manufacturing – Now a days, computer networks are used i several aspects of manufacturing, including the manufacturing process itsel Two applications which use a network to provide necessary services an computer-assisted manufacturing (CAM) and computer-assisted design (CAD) both of which permit multiple users to work on a project simultaneously.

(iii) Financial Services – In present, financial services ar completely dependent on computer networks. Main applications are credi history searches, foreign exchange and investment services, and Electron Funds Transfer (EFT) that permits a user to transfer money without goi into a bank.

(iv) Teleconferencing – With the help of teleconferencing conferences are possible to occur without the participants being in the sam place. Applications include simple text conferencing, voice conferencing, an video conferencing.

(v) Cable Television – Future services provided by cable televisio networks can include video on request, as well as the same information, financi and communications services currently provided by the telephone companie and computer networks.

(vi) Information Services – Network information services includ bulletin boards and data banks. A World Wide Web site offering the technic specifications for a new product is an information service.

(vii) Electronic Messaging – Electronic mail (e-mail) is the mo widely used network application.

(viii) Electronic Data Interchange (EDI) – EDI permits busines information to be transferred without using paper.

(ix) Directory Services – By using directory services, it is possible t store the list of files in a central location to speed worldwide search operation

(x) Cellular Telephone – In the past, two parties desiring to use the services of the telephone company had to be linked by a fixed physical connection. But, in present cellular networks make it possible to maintain wireless phone connections even while traveling over large distances.

Q.5. What are the components of computer network ? Explain goals of computer network. ***(R.G.P.V., June 2012)***

Ans. The basic components of computer network are shown in fig. 1.1. All computer networks include some combination of the following – end stations, applications, and a network that will support the data traffic between the end stations. A computer network designed a few years ago to support the basic networking applications of the time may have a difficult time supporting recently developed high-end applications, such as medical imaging and live video teleconferencing. Network designers, administrators, and managers must understand and monitor the most recent types and frequency of networked applications.

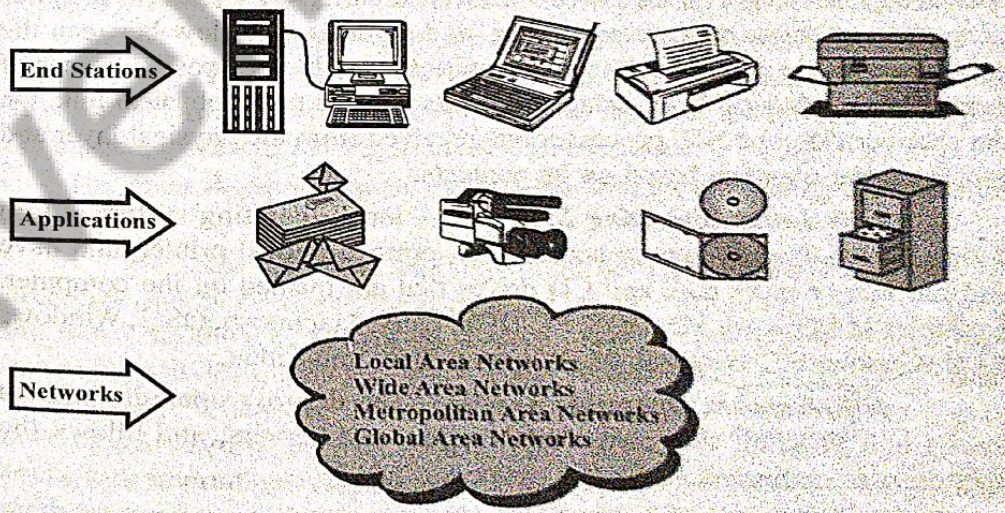


Fig. 1.1 Basic Network Components

Computer network share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other peripherals hardware and software resources, network interface card (NIC), local operating system (LOS), and the network operating system (NOS).

(i) Servers – Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communications servers, database servers, directory/ security servers, fax servers and web servers, to name a few.

(ii) Clients – Clients are computers that access and use the network and shared network resources. Client computers are basically the customer (users) of the network, as they request and receive services from the server.

(iii) Transmission Media – Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair cable, coaxial cable, and optical fibre cable. Transmission media are sometimes called channels, links, or lines.

(iv) Shared Data – Shared data are data that file servers provide to clients, such as data files, printer access programs, and e-mail.

(v) Shared Printers and Other Peripherals Hardware and Software resources – Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

(vi) Network Interface Card – In a network, each computer has a special expansion card called a network interface card (NIC). The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmitter side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver side, the NIC processes bits received from the physical layer and processes the message based on its contents.

(vii) Local Operating System – A local operating system (LOS) allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples of LOSs are MS-DOS, PC-DOS, Unix, Macintosh, OS/2, Windows 3.11, Windows 95, Windows 98, Windows 2000 and Linux.

(viii) Network Operating System – The network operating system (NOS) is a program that runs on computers and servers, and allows the computers to communicate over a network.

Goals – Refer the ans. of Q.3.

Q.6. What are the different topologies used in computer networks? Explain. ***(R.G.P.V., May/June 2004)***

Ans. The term topology refers to the way a network is laid out, either physically or logically. The connection of two or more devices forms a link and two or more links forms a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices to one another. Basically, there are five topologies – mesh, star, tree, bus, and ring.

(i) Mesh – Every device has a dedicated point-to-point link to each other devices in a mesh topology. Therefore a fully connected mesh network has n(n – 1)/2 physical channels to link n devices. Each device on the network must have (n – 1) input/output ports to accomodate that every links (see fig. 1.2).

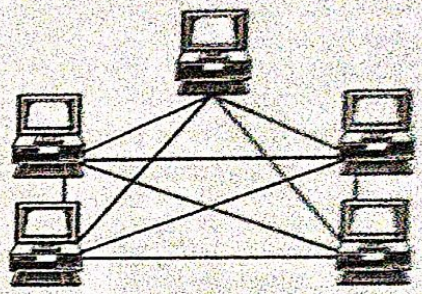


Fig. 1.2 Fully-connected Mesh Topology

Mesh topology has several advantages –

(a) The use of dedicated links guarantees that each connection can carry its own data load, therefore minimizing the traffic problems which can take place if links must be shared by multiple devices.

(b) It is robust. It does not incapacitate the entire system when one link damages.

(c) It enforces privacy or security. When every add sent message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

(d) The point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and helps in finding its cause and solution.

The main disadvantage of mesh is the amount of cabling and I/O ports required.

(ii) Star – In a star topology every device has a dedicated point-to-point link only to a central controller called the hub. The devices cannot be directly linked to each other, but the controller acts as exchange. When one device wants to send data to another, it sends the data first to the hub which then relays it to the other device connected to it (see fig 1.3).

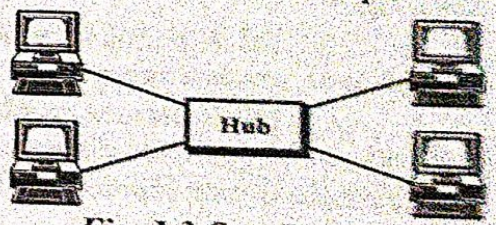


Fig. 1.3 Star Topology

The advantages of star topology are –

(a) It is less expensive as compared to mesh.

(b) Every device requires only one link and one I/O port to connect it to any number of others. This makes it easy to install and reconfigure.

(c) Less cabling is required.

(d) Easy to add, delete, or move devices as it involves only one connection between a device and hub.

(e) Robustness; it implies that if one link fails, only that link is affected other links remain active.

However, it needs more cabling than tree, ring, or bus topologies.

(iii) Tree – A variation of a star topology is a tree topology. Nodes in tree are linked to the central hub as is done in star but every device is not directly plugged into central hub. The majority of devices connect to a secondary hub that in turn is connected to the central hub as shown in fig. 1.4.

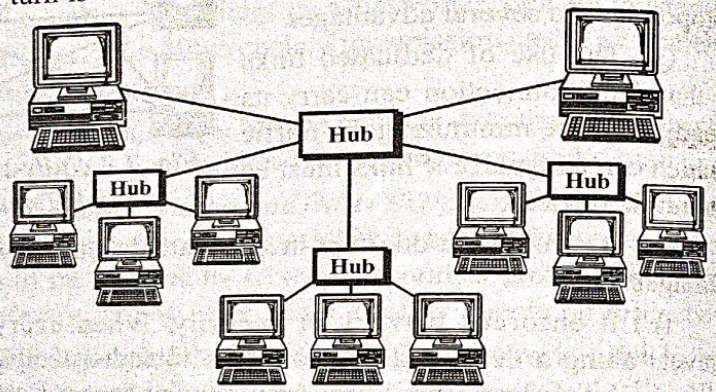


Fig. 1.4 Tree Topology

In a tree topology, the central hub is active hub which contains a repeater to strengthen the transmission and to increase the distance a signal can travel. The secondary hubs can be active or passive hubs. A simple physical connection between the attached devices is provided by a passive hub.

Generally, the advantages and disadvantages of a tree topology are the same as those of a star. But, the addition of secondary hubs adds two more advantages –

(a) It permits the network to isolate and prioritizes communications from various computers.

(b) It permits more devices to be attached to a single central hub and can increase the distance a signal can travel between devices.

Example of tree topology is cable TV technology.

(iv) Bus – A bus topology describes a multipoint configuration. One long cable acts as a backbone to link all the devices in the network.

Nodes are connected to the bus cable by drop lines and taps as shown in fig. 1.5. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker the farther it has to travel. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantage of bus topology is ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. Also, bus uses less cabling than mesh, star or tree topologies.

Disadvantages include difficult reconfiguration and fault isolation. A bus is usually designed to be optimally efficient at installation. It

poses difficulty to add new devices. Also, signal reflection at the taps can cause degradation in quality which can be controlled by limiting the number of taps and spacing. In addition, faults and break in the bus cable stop all transmission.

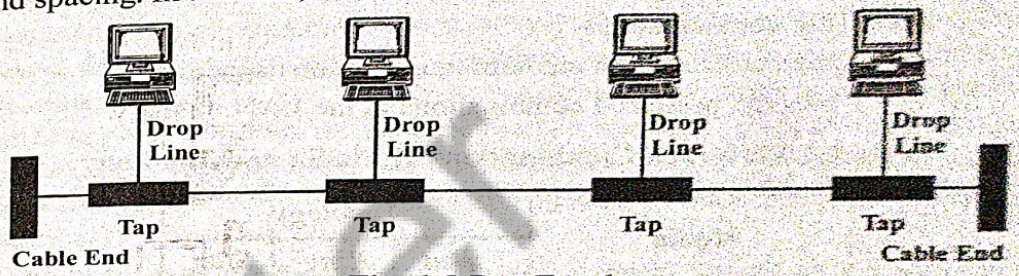


Fig. 1.5 Bus Topology

(v) Ring – Every device has a dedicated point-to-point line configuration only with the two devices on either side of it in ring topology. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device has a repeater which regenerates the bits and passes them along to another device as shown in fig. 1.6.

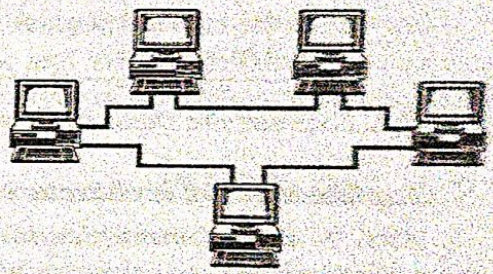


Fig. 1.6 Ring Topology

The major advantages of ring topology are as follows –

(a) It is easy to install and reconfigure.

(b) It is easy to add or delete a device as it requires to move only two connection.

(c) Fault isolation is simplified.

The major constraints are –

(a) The media and traffic considerations (maximum length and number of devices).

(b) Unidirectional traffic can also be a demerit as a break in the ring can disable the entire network.

Q.7. Why star topology is commonly preferred ? (R.G.P.V., Dec. 2016)

Ans. Refer the ans. of Q.6 (ii).

Q.8. What are the various network topologies ? List the factors that affect the choice of a topology and transmission medium in a LAN. (R.G.P.V., June 2012)

Ans. **Network Topologies** – Refer the ans. of Q.6.

Factors Affecting the Choice of a Topology and Transmission Medium in a LAN – The choices of transmission medium and topology depend on

each other. Some media are appropriate for point-to-point rather than point-to-multipoint transmission. Other considerations for choice of medium for topology are as follows –

(i) Cost considerations

(ii) Underutilization of medium transmission capacities.

Table 1.1 lists the preferred combinations in the LAN industry.

Table 1.1 Preferred Combinations of Media and Topology

Media	*Topology*		
	Bus	*Ring*	*Star*
Twisted pair	✓	✓	✓
Baseband coaxial	✓	✓	
Broadband coaxial	✓		
Optical fibre		✓	

Q.9. Explain the theoretical view of a computer network architecture.

Or

Explain network architecture in detail. ***(R.G.P.V., May 2015)***

Ans. A ***data communication network*** is any system of computers, computer terminals, or computer peripheral equipments used to transmit and/or receive information between two or more locations. ***Network architecture*** outline the products and services necessary for the individual components within a data communication network to operate together.

Network architecture is a set of equipment, transmission media, and procedures that ensures that a specific sequence of events occurs in a network in the proper order to produce the intended results. Network architecture must include sufficient information to allow a program or a piece of hardware to perform its intended function. The primary goal of network architecture is to give the users of the network the tools necessary for setting up the network and performing data flow control. A network architecture outlines the way in which a data communication network is arranged or structured and generally includes the concept of ***levels*** or ***layers*** of functional responsibility within the architecture. The ***functional responsibilities*** include electrical specifications, hardware arrangements, and software procedures.

Networks and network protocols fall into three general classifications: ***current, legacy*** and ***legendary.*** Current networks include the most modern and sophisticated networks and protocols available. If a network or protocol becomes a legacy, no one really wants to use it, but for some reason it just will not go away. When an antiquated network or protocol finally disappears, it becomes legendary.

In general terms, computer networks can be classified in two different ways – ***broadcast*** and ***point-to-point.*** With broadcast networks, all stations and devices on the network share a single communications channel. Data are propagated through the network in relatively short messages sometimes called ***frames***, ***blocks***, or ***packets.*** Many or all subscribers of the network receive transmitted messages, and each message contains an address that identifies specifically which subscriber (or subscribers) is intended to receive the message. When messages are intended for all subscribers on the network, it is called broadcasting, and when messages are intended for a specific group of subscribers, it is called ***multicasting.***

Point-to-point networks have only two stations. Therefore, no addresses are needed. All transmissions from one station are intended for and received by the other station. With point-to-point networks, data are often transmitted in long, continuous messages, sometimes requiring several hours to send.

In more specific terms, point-to-point and broadcast networks can be subdivided into many categories in which one type of network is often included as a subnetwork of another.

Q.10. What is multicasting ? ***(R.G.P.V., June 2015)***

Ans. Refer the ans. of Q.9.

Q.11. What do you mean by broadcast network ? Discuss the need or lack of need for a network layer (OSI layer) in a broadcast network. ***(R.G.P.V., June 2017)***

Ans. Broadcast networks have a single communication channel that is shared by all the machines on the network. Short messages, called packets in certain contexts, sent by any machine are received by all the others. An address field within the packet specifies for whom it is intended. Upon receiving a packet, a machine checks the address field. If the packet is intended for itself, it processes the packet, if the packet is intended for some other machine, it is just ignored.

Broadcast systems generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting. Some broadcast systems also support transmission to a subset of the machines, something known as multicasting. One possible scheme is to reserve one bit to indicate multicasting. The remaining $n - 1$ address bits can hold a group number. Each machine can "subscribe" to all machines subscribing to that group.

Broadcast network is another name for a shared-medium LAN. Because it is a "broadcast network" means only that every station sees every packet and therefore every station must decide to accept or ignore every packet that it sees.

The network layer, or OSI layer 3, or IP in a TCP/IP system, provid station-to-station addressing of packets. This function is necessary both f transmission and reception functions.

Q.12. Briefly describe the major network classifications.

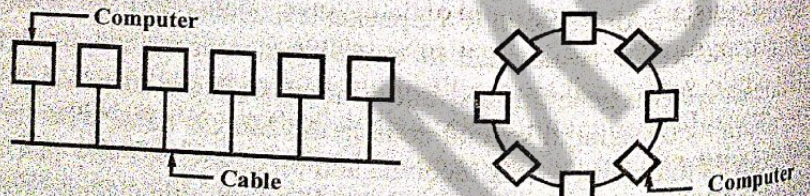
Ans. Networks are generally classified by size, which includ geographic area, distance between stations, number of computer transmission speed (bps), transmission media, and the network's physic architecture. The three primary classifications of networks are local ar networks (LANs), metropolitan area neworks (MANs), wide area networ (WANs) af follows –

(i) Local Area Networks (LANs) – A local area network (LAN) usually privately owned and links the devices in a single office, building campus. Depending on the requirements of an organization and the type technology used, a LAN can be as simple as two PCs and a printer in someone home office, or it can extend throughout a company and includes voice, sour and video peripherals. LANs are differentiated from other types of networ by three characteristics –

(a) Their size (b) Their transmission technology (c) Their topolog

Size of the LANs is restricted. It means that the worst-case transmissio time is bounded and known in advance. By knowing this bound, it becom possible to use certain types of designs which would not otherwise be possibl It also simplifies network management.

LANs often use a transmission technology which consists of a sing cable to which all the machines are connected, like the telephone compa party lines once used in rural areas. Traditional LANs run at speeds of 10 100 Mbps, have low delay (tens of microseconds), and make very few erro



(a) Bus ***(b) Ring***

Fig. 1.7 Various Topologies

To broadcast LANs many topologies are possible. Two of them are show in fig. 1.7. In a bus topology, at any moment one machine is the master and permitted to transmit. All other machines are needed to refrain from transmitti If two or more machines want to transmit simultaneously, an arbitrati mechanism is required to resolve conflicts. Arbitration mechanism can centralized or distributed.

Ring is the second type of broadcast system. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Each bit circumnavigates the whole ring in the time it takes to send some bits, often before the complete packet has even been sent.

Other type of LAN is built using point-to-point lines. Individual lines connect a specific machine with another specific machine. This type of LAN is really a miniature wide area network.

A local area network is generally a private owned communications network within a confined geographical area. The range is usually within a few kilometres. (less than 10 km) – may be one office, one building or a group of buildings located closely such as a college campus. The transmission channels generally use coaxial or fibre optic cables and special interface units rather than telephone lines and modems.

(ii) Metropolitan Area Networks (MANs) – A metropolitan area network (MAN) is basically a bigger version of a LAN and normally uses similar technology. It is designed to extend over an entire city. It may be a single network such as a cable television network or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device. A key aspect of a MAN is that there is a broadcast medium to which all the computers are attached, due to which the design is greatly simplified as compared to there type of networks.

A MAN can support both data and voice, and might even be related to the local cable television distribution network. It might cover a group of nearby offices or a city and might be either private or public. A MAN just has one or two cables and does not contain switching elements.

(iii) Wide Area Networks (WANs) – Wide area network (WAN) provides long-distance transmission of data, voice, image and video information over large geographical areas that may comprise a country, a continent, or even the whole world. It has a collection of machines intended for running user programs. These machines are called ***hosts***. Hosts are connected by a ***communication subnet*** or just ***subnet***. The subnet carries messages from host-to-host. By separating the pure communication aspects of the network (subnet) from the application aspects (hosts), the complete network design is greatly simplified.

There are two distinct components of the subnet namely, most wide area networks which are transmission lines and switching elements. Transmission lines move bits between machines. Switching elements are specialized computers which are used to connect two or more transmission lines.

In most WANs, the network has numerous cables or telephone lines, each one connecting a pair of routers. When two routers which do not share

a cable wish to communicate, they must perform this indirectly, via other routers. When a packet is transmitted from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the needed output line is free, and then forwarded. A subnet using this principle is known as a ***point-to-point***, ***store-and-forward***, or ***packet-switched*** subnet.

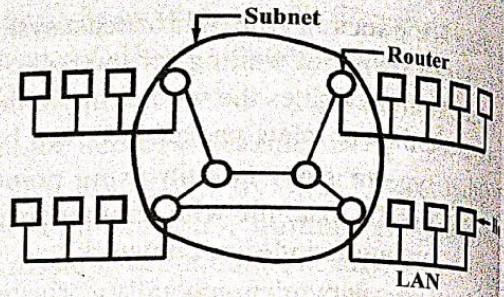


Fig. 1.8 Relation between Hosts on LAN and Subnet

A WAN can be a public system such as the Public Switched Telephone Network (PSTN) or one of the various packet switched services provided by the public telecommunication authorities. WAN can also use most other types of circuits including satellite networks, ISDN, ATM, Value Added Networks. The main distinguishing feature between a LAN and a WAN is that the LAN is under the complete control of the owner.

Q.13. Describe and differentiate LAN and WAN. (R.G.P.V., June 20

Ans. **LAN and WAN** – Refer the ans. of Q.12.

Differences between LAN and WAN –

(i) The scope of LAN is small, typically a single building or a cluster of buildings whereas a WAN spans a large geographical area, often a country or continent. This difference in geographic scope leads to different technical solutions.

(ii) LAN is usually owned by the same organization that owns the attached devices. For WAN's this is less often, a significant fraction of the network assets are not owned. This has two implications –

(a) Care must be taken in the choice of LAN, because there may be a substantial capital investment for both purchase and maintenance.

(b) The network management responsibility for a LAN falls solely on the user.

(iii) The internal data rates of LANs are typically much greater than those of WANs.

(iv) In a LAN, the computers, terminals and peripheral devices are usually physically connected with wires and coaxial cables. Whereas, in a WAN, there may not be a direct physical connection between various computers.

(v) The cost to transmit data in a LAN is negligible because the transmission medium is usually owned by the user organization. However, in case of a WAN, this cost may be very high because the transmission media

used are leased lines or public systems such as telephone lines, microwave and satellite links.

(vi) Fewer data transmission errors occur in case of a LAN as compared to a WAN. This is mainly because in case of a LAN, the distance covered by the data is negligible as compared to a WAN.

LAYERED ARCHITECTURE – PROTOCOL HIERARCHY, DESIGN ISSUES, INTERFACES AND SERVICES, CONNECTION-ORIENTED & CONNECTIONLESS SERVICES, SERVICE PRIMITIVES, DESIGN ISSUES & ITS FUNCTIONALITY

Q.14. What is protocol ? ***(R.G.P.V., Dec. 2016)***

Ans. A protocol is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions. They are free to change their protocols at will, provided they do not change the service visible to their users. In this way, the service and the protocol are completely decoupled.

Q.15. Discuss layered network architecture. ***(R.G.P.V., Dec. 2009)***

Ans. Layering is a widely accepted structuring technique in designing a communication system. A set of layers and protocols is called a network architecture. To reduce their design complexity, networks are organized as a series of layers, each one built on the layer below it. The number of layers, their contents and their functions varies from network to network. However, in all networks, the purpose of each layer is to offer certain services to the higher layers, protecting those layers from the implementation details of services.

The communication between the two machines or parties is done by protocols. A protocol is defined as a set of rules governing the exchange of data between two separate entities or application programs. For two entities to communicate successfully they must speak the same language i.e., they must follow the same set of conventions when they decide what to communicate, when to communicate and how to communicate. These conventions when standardized are called protocols. Violating the protocol will make communication more difficult, if not impossible.

A five layer network is shown in the fig. 1.9. Layer 'N' on one machine carries on a conversation with layer N on another machine. The rules and conventions used in this conversation are collectively known as the layer N protocol. The entities forming corresponding layers on different machines are called peer processes. Thus, peer processes communicate with each other using the protocol at that level.

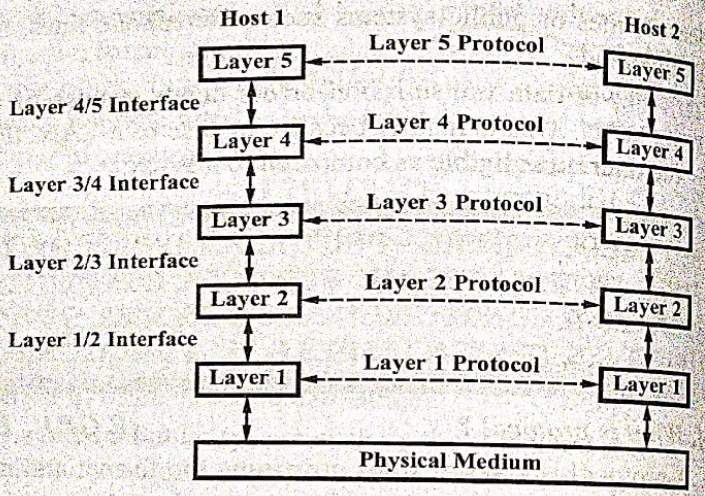


Fig. 1.9 Layers, Protocols and Interfaces

A process communicates with other processes situated above below it in adjacent layers through an interface. There is an interface betw each pair of adjacent layers. The interface is realized as one or more ser access points or SAPs. The process at layer N – 1 provides a servic the N^{th} layer through the request of a primitive. A primitive specifie function to be performed and is also used to pass data and con information.

In reality, there is no direct data transfer between layer N on one mach and its peer process on another machine. Instead, each layer passes data control information to the layer immediately below it, until the lowest lay reached. Below layer 1 is the physical medium through which ac communication occurs. In fig. 1.9, physical communication is indicate solid lines and virtual communication by deshed lines.

Q.16. List the major advantages with the layered approach to prot ***(R.G.P.V., Dec.***

Or

Write the advantages of layered architecture of a computer netwo ***(R.G.P.V., Dec.***

Or

What are the reasons of using layered protocol ? (R.G.P.V., June

Ans. Advantages of layered approach are as follows –

(i) Layering reduces the design complexity of the network.

(ii) In a layered architecture, each layer functions to independent of the neighbouring layers, so any technological changes layer at any time can be easily incorporated.

(iii) Since the functionality of layers is independent so each layer can follows its independent protocol as per its requirements.

(iv) Layering facilitates troubleshooting and reduces maintenance complexity.

(v) Layering helps in message format conversions between different protocols followed at different/same layers.

(vi) Layering facilitates internationally standardized working.

(vii) Layering helps in proper division of work to achieve the overall objective of proper communication.

Q.17. What are two reasons for using layered protocols ? What is one possible disadvantage of using layered protocols ? (R.G.P.V., Dec. 2015)

Ans. **Reasons for using Layered Protocols** – Refer the ans. of Q.16.

Disadvantage – The major disadvantage of using a layered network model is that it is somewhat inefficient. Because there are several layers, each with its own software and packets, sending a message involves many software programs and many packets.

Q.18. What do you mean by interfaces and services ? Also discuss protocol data unit.

Ans. In every layer, the active elements are often known as entities. An entity can be a hardware entity (such as an intelligent I/O chip) or a software entity (such as a process). In the same layer on different machines, entities are known as peer entities. The entities in layer N implement a service used by layer N + 1. For this case, layer N is known as service provider and layer N + 1 is known as service user. In order to provide its service, layer N can use the services of layer N – 1. It may offer various service classes, for example, slow, cheap communication and fast, expensive communication.

At service access points (SAPs), services are available. The layer N SAPs are the places in which layer N + 1 can access the services offered. Every SAP has an address which uniquely identifies it. In the telephone system, the SAPs are the sockets into which modular telephones can be plugged to make this point clearer and the SAP addresses are the telephone numbers of these sockets. We must know the callee's SAP address to call someone. In similar way, the SAP addresses are street addresses and post office box numbers in the postal system. To sent a letter, we must know the addressee's SAP address.

There has to be an agreed upon set of rules about the interface in order for two layers to exchange information. Fig. 1.10 shows the layer N + 1 entity passes an IDU (Interface Data Unit) to the layer N entity through the SAP at a typical interface. The IDU made up of an SDU (Service Data Unit) and some control information. The SDU is the information passed across the network to

the peer entity and then up to layer N + 1. The control information is requ
to help the lower layer do its Job but is not part of the data itself.

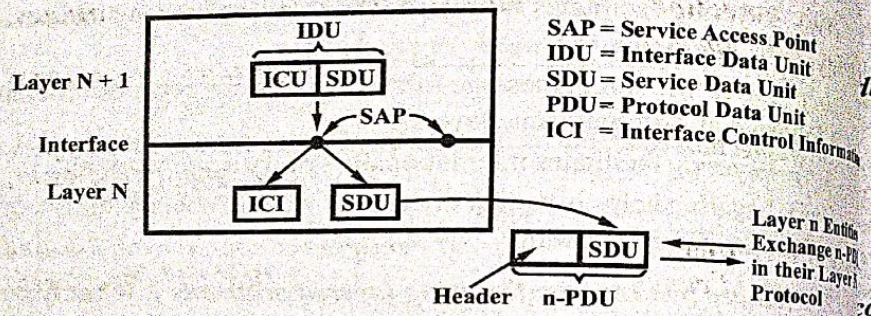


Fig. 1.10 Relation between Layers at an Interface

In order to transfer the SDU, the layer n entity may have to fragme into several pieces, each of which is given a header and transmitted separate PDU (Protocol Data Unit) like a packet. The peer entities us PDU headers to carry out their peer protocol. They identify which Pl contain data and which contain control information, give sequence num and counts, and so on.

Q.19. Explain interfaces and services. ***(R.G.P.V., Dec. 1***

Ans. Refer the ans. of Q.18.

Q.20. Explain the term services, interfaces and protocol in details. the relationships between services and protocols. ***(R.G.P.V., Dec. 2***

Ans. Refer the ans. of Q.18 and Q.14.

Relationships between Services and Protocols – A service is a s primitives (operations) that a layer gives to the layer above it. The ser defines what operations the layer is prepared to perform on behalf of its u but it says nothing at all about how these operation are implemented. A ser relates to an interface between two layers, with the lower layer being service provider and the upper layer being the service user.

An analogy with programming languages is worth making. In obj oriented language, a service is like an abstract data type or an object. It de operations which is performed on an object but does not specify how operations are implemented. A protocol relates to the implementation o service and as such is not visible to the user of the service.

Many older protocols did not distinguish the service from the prot In effect, a typical layer might have had a service primitive SEND PAC with the user providing a pointer to a fully assembled packet. This arrange meant that all changes to the protocol were immediately visible to the Most network designers now regard such a design as a serious blunder.

Q.21. Explain the working of –
(i) Connection-oriented and
(ii) Connectionless services. What are their advantages, disadvantages and applications ?
(R.G.P.V., June 2014)

Or

Explain connection-oriented and connectionless services with examples.
(R.G.P.V., Dec. 2009, June 2012)

Or

What is the difference between connectionless communication and connection-oriented communication ? ***(R.G.P.V., Dec. 2016)***

Or

What is the principle difference between connectionless communication and connection-oriented communication ? (R.G.P.V., Dec. 2012, June 2016)

Or

Compare connectionless and connection-oriented services.
(R.G.P.V., Dec. 2010)

Or

Write any two differences between connection-oriented and connectionless services. ***(R.G.P.V., June 2015)***

Or

Differentiate between connectionless and connection-oriented services of networks. ***(R.G.P.V., Dec. 2015)***

Or

Differentiate between connectionless and connection-oriented services. Discuss their advantages, disadvantages and typical applications.
(R.G.P.V., Dec. 2017)

Ans. Connection-oriented communication has three phases. In the establishment phase a request is made to set up a connection. Only after this phase has been successfully completed can the data transfer phase be started and data transported. Thereafter the release phase comes connectionless communication does not have three phases. It just sends the data.

Connection-oriented service is modeled after the telephone system. To talk to someone we pick up the phone, dial the number, talk and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection. The essential aspect of a connection is that it acts like a tube – the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end. In most cases, the order is preserved so that the bits arrive in the order they were sent.

In some cases, when a connection is established, the sender, receiver and subnet conduct a negotiation about parameters to be used, such as maximum message size, quality of service required, and other issues. Typically, one side makes a proposal and the other side can accept it, reject it, or make a counter proposal.

The advantage of connection-oriented networking lies in its guara
capacity. Once a circuit is established, no other network activity will de
the capacity of that circuit. One disadvantage of connection-or
technology is due to cost – circuit costs are fixed, independent of u
instance, one pays a fixed rate for a phone call, even when the two
do not talk.

In contrast, ***connectionless service*** is modeled after the postal
Each message (letter) carries the full destination address, and each
routed through the system independent of all the others. Normally, wh
messages are sent to the same destination, the first one sent will be
one to arrive. However, it is possible that the first one sent can be dela
that the second one arrives first.

The main advantage of connectionless service is that mu
communications among computers can proceed concurrently,
intermachine connections shared by all pairs of computers th
communicating. The disadvantage is that as activity increases, a given
communicating computers receives less of the network capacity. Th
whenever a connectionless network becomes overloaded, computers
the network must wait before they can send additional packets.

Each service can be characterized by a quality of service. Some se
are reliable in the sense that they never lose data. Usually, a reliable s
is implemented by having the receiver acknowledge the receipt of
message so the sender is sure that it arrived. The acknowledgement
introduces overhead and delays, which are often worth it but are som
undesirable.

A typical situation in which a reliable connection-oriented ser
appropriate is file transfer. The owner of the file wants to be sure that
bits arrive correctly and in the same order they were sent. Very few file tr
customers would prefer a service that occasionally scrambles or loses
bits, even if it is much faster.

There are two minor variations in reliable connection-oriented ser
message sequences and byte streams. The message boundaries are pre
in the former. If two 1-KB messages are sent, they arrive as two distinct
messages, never as one 2-KB message. In the latter, the connection is a
of bytes having no message boundries. If 2K bytes arrive at the receiver
is no way to tell if they were sent as one 2 KB message, two 1-KB mes
or 2048 1-byte messages. It might be important to preserve the m
boundaries when the pages of a book are sent over a netwo
phototypesetter as separate messages. On the contrary, with a terminal
into a remote timesharing system, a byte stream from the terminal
computer is all that is required.

The delays introduced by acknowledgements are unacceptable for some
pplications. The digitized voice traffic is such an application. For telephone
sers, it is preferable to hear a bit of noise on the line or a garbled word from
ime-to-time than to introduce a delay to wait for acknowledgements. Likewise,
hen transmitting a video film, having a few pixels wrong is no problem, but
aving the film jerk along as the flow stops to correct errors is immensely
rritating.

All applications do not need connections. For instance, as electronic mail
ecomes more common, can electronic junk mail be far behind ? Probably, the
lectronic junk mail sender does not need to go to the trouble of setting up and
ater tearing down a connection to send one item. Nor is 100 percent reliable
elivery especially if it costs too much. All that is required is a way to send a
ingle message that has a high probability of arrival, but no quarantee. Unreliable
onnectionless service is known as datagram service, in analogy with telegram
ervice, which also does not send an acknowledgement back to the sender.

In other cases, the convenience of not having to establish a connection to
end one short message is needed, but reliability is necessary. For these
pplications, the acknowledged datagram service can be offered. It is similar
o sending a registered letter and requesting a return receipt to sure that the
etter was delivered to the intended party.

Another service is the request-reply service. In this service, the sender
ransmits a single datagram containing a request. The reply has the answer.
or instance, a query to the local library asking where Uighur is spoken comes
n this category.

In the client-server model, the request-reply is used to implement
ommunication. Table 1.2 lists these types of services.

Table 1.2 Six Different Kinds of Services

	Service	*Example*
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Q.22. Two networks each provide reliable connection-oriented service. One of them offers a reliable byte stream and the other offers a reliable message stream. Are these identical ? If so, why is distinction made ? If not, given an example of how they are differ ? ***(R.G.P.V., May 2018)***

Ans. Refer the ans. of Q.21.

Q.23. Write down the service primitives for implementing a co... network.

Ans. A service is formally specified by a set of primitives (ope... available to a user process to access the service. These primitives t... service to perform some actions or reports on an action taken by a pee... The primitives are normally system calls when the protocol stack is loc... the operating system. These calls cause a trap to kernel mode, whic... turns control of the machine over to the operating system to transm... necessary packets.

The set of primitives available depends on the nature of the servic... provided. For connection-oriented service, the primitives are differen... those of connectionless service. As a minimal example of the service pro... that might be provided to implement a reliable byte stream in a client... environment, consider the primitives listed in fig. 1.11.

Primitive	*Meaning*
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Fig. 1.11 Five Service Primitives for Implementing a Simple Connection-oriented Service

These primitives might be used as follows. First, the server exe... LISTEN to indicate that it is prepared to accept incoming connecti... common way to implement LISTEN is to make it a blocking system ca... server process is blocked until a request for connection appears after exe... the primitive.

Next, the client process executes CONNECT to establish a conn... with the server. The CONNECT call needs to specify who to connect t... might have a parameter giving the server's address. The operating s... then typically sends a packet to the peer asking it to connect, as shown... in fig. 1.12. The client process is suspended until there is a response... the packet arrives at the server, it is processed by the operating system... When the system sees that the packet is requesting a connection, it chec... see if there is a listener. If so, it does two things – unblocks the listen... sends back an acknowledgement (2). The arrival of this acknowledg... then releases the client. At this point, the client and server are both runn... they have a connection established. It is important to note th... acknowledgement (2) is generated by the protocol code itself, not in re...

...a user-level primitive. If a connection request arrives and there is no listener, ...e result is undefined. In some systems, the packet may be queued for a ...hort time in anticipation of a LISTEN.

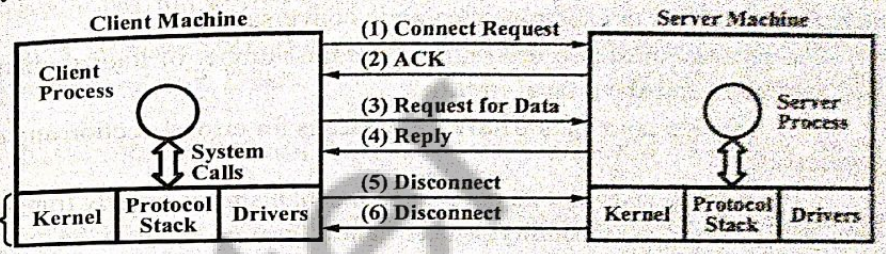


Fig. 1.12 Packets Sent in a Simple Client-server Interaction on a Connection-oriented Network

The next step is for the server to execute RECEIVE to prepare to accept ...e first request. Normally, the server does this immediately upon being released ...om the LISTEN, before the acknowledgement can get back to the client. ...he RECEIVE call blocks the server.

Then the client executes SEND to transmit its request (3) followed by the ...xecution of RECEIVE to get the reply.

This arrival of the request packet at the server machine unblocks the ...erver process so it can process the request. After it has done the work, it ...ses SEND to return the answer to the client (4). The arrival of this packet ...nblocks the client, which can now inspect the answer. If the client has ...dditional requests, it can make them now. If it is done, it can use ...ISCONNECT to terminate the connection. Usually, an initial DISCONNECT ... a blocking call, suspending the client and sending a packet to the server ...aying that the connection is no longer needed (5). When the server gets ...e packet, it also issues a DISCONNECT of its own, acknowledging the ...lient and releasing the connection. When the server's packet (6) gets ...ack to the client machine, the client process is released and the connection ... broken.

Q.24. Describe the design issues for the layers. (R.G.P.V., June 2010, 2012)

Ans. Some of the key design issues are listed below –

(i) Every layer needs a mechanism for identifying transmitters and ...eceivers. Because a network generally contain several computers, some form ...f addressing is needed in order to specify a specific computer.

(ii) Decision should be made about the rules for data transfer. Among ...he following three modes of data communication one may be selected.

(a) Simplex Communication – Data only travels in one ...irection. For example, home television set.

(b) Half-duplex Communication – Data can travel in direction, but not simultaneously. For example, wireless.

(c) Full-duplex Communication – Data travels in directions at once. For example, telephonic conversation.

The protocol must also determine about the number of logical ch per connection and about their priorities.

(iii) The layer should have some means for error detection and correction.

(iv) The layer should have some mechanism for orderly trans data. This involves the capability to piece data at one end and join the pi other end.

(v) There should be a mechanism for flow control and conge control.

(vi) There should be enough means to multiplex the data from communicating processes, over the same physical circuit.

(vii) The layers must have mechanism for deciding about the of service (request) reply, reliable, priority, etc.

(viii) There must be a mechanism to make routing decisions i there are multiple paths between source and destination.

ISO-OSI REFERENCE MODEL – PRINCIPLE, MODEL, DESCRIPTIONS OF VARIOUS LAYERS AND ITS COMPARISON WITH TCP/IP

Q.25. What are the principles used in defining the OSI layer?

Ans. The principles that were applied to arrive at the seven layer laid down by ***Day and Zimmermann*** in 1983, are as follows –

(i) Each layer should perform a well defined function.

(ii) A layer should be created where a different level of abst is required.

(iii) The function of each layer should be selected with towards defining internationally standardized protocols.

(iv) The layer boundaries should be selected to minim information flow across the interfaces.

(v) The number of layers should be large enough that functions need not be thrown together in the same layer out of neces small enough that the architecture does not become unwieldy.

(vi) Allow changes of functions of protocols to be made layer without affecting other layers.

Q.26. Explain the principles that were applied at the time of seven layer architecture design of ISO-OSI reference model. ***(R.G.P.V., May 2018)***

Ans. Refer the ans. of Q.25.

Q.27. Explain ISO/OSI model with well labelled diagram and explain the function of each layer. ***(R.G.P.V., June 2009)***

Or

Explain the OSI model in detail. ***(R.G.P.V., Dec. 2010, 2012)***

Or

Explain the ISO-OSI model of computer network. Give the function of each layer. ***(R.G.P.V., June 2014)***

Or

During the communication, how various layers of OSI model exchange information to establish a connection ? Describe with the help of a suitable diagram. ***(R.G.P.V., June 2015)***

Or

Draw the layered architecture of OSI reference model. Also explain function of each in brief. ***(R.G.P.V., Dec. 2015)***

Ans. International Standards Organization (ISO) in 1983, developed this model as a first step toward international standardization of the protocols used in the various layers. As it deals with connecting open systems, that is, systems that are open for communication with other systems, the model is called the ***ISO-OSI (Open System Interconnection) Reference Model.***

OSI is a layered framework for the design of network systems which permit for communication across all types of computer systems. It has seven separate but related layers, each of which defines a segment of the process of moving information across a network.

The OSI model is shown in fig. 1.13. (physical medium is not shown). The OSI model has seven layers.

The functions of each layer are given as follows –

(i) Physical Layer – This layer coordinates the functions needed to send a bit stream over a physical medium. It deals with the electrical and mechanical specifications of the interface and transmission medium. It also expresses the procedures and functions which physical devices and interfaces have to perform for transmission to take place. The physical layer is related with the following –

(a) Representation of Bits – Physical layer data have a stream of bits (sequence of 0s and 1s) without any interpretation. For transmission, bits should be encoded into signals – electrical or optical. The type of encoding is defined by the physical layer.

Vernier

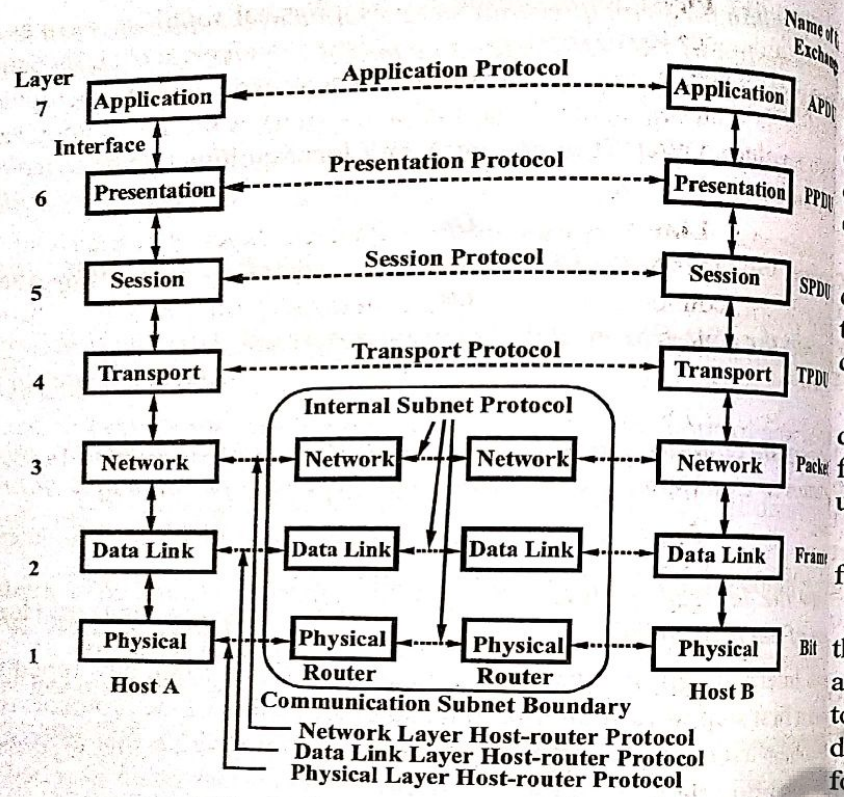


Fig. 1.13 The OSI Reference Model

(b) Synchronization of Bits – At the bit level, transmitter and receiver should be synchronized. In another way, transmitter and receiver clocks should be synchronized.

(c) Transmission Mode – The direction of transmission between two devices – simplex, half-duplex or full-duplex are defined in physical layer. Simplex mode is a one way communication in which one can only send and other can only receive. In the case of ***half-duplex*** two devices can send and receive but not at the same time. For two devices sending and receiving at the same time, a ***full duplex*** (or simply duplex) is used.

(d) Physical Characteristics of Interfaces and Media – characteristics of the interface between the devices and transmission are defined by the physical layer. Physical layer also defines the transmission medium.

(e) Data Rate – Physical layer also defines the number sent each second which is known as transmission rate. In the other the duration of a bit is defined by the physical layer, that is how long

(f) Physical Topology – The physical topology defines the connection of devices to make a network. Devices can be attached by using a star topology (devices are connected through a central device), a ring topology (each device is attached to the next, making a ring), a mesh topology (each device connected to every other device), or a bus topology (each device on a common link).

(g) Line Configuration – Physical layer is related with the connection of devices to the medium. In case of point-to-point configuration, two devices are connected together by a dedicated link. In the multipoint configuration, a link is shared between many devices.

(ii) Data Link Layer – The physical layer is transformed by the data link layer, a raw transmission facility, to a reliable link and is responsible for node-to-node delivery. It makes the physical layer appears error free to the upper layer. The main functions of data link layer are the following –

(a) Framing – Data link layer divides the bits stream received from the network layer into manageable data units known as ***frames***.

(b) Physical Addressing – The data link layer adds a header to the frame to define the physical address of the transmitter (source address) and receiver (destination address) of the frame when frames are to be distributed to various systems on the network. The receiver address is the address of the device which connects one network to the next when the frame is intended for a system outside the sender's network.

(c) Flow Control – When the rate at which the data are absorbed by the receiver is less than the rate generated in the transmitter, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.

(d) Error Control – By adding mechanisms to detect and retransmit damaged or lost frames, the data link layer adds the reliability to the physical layer. It also employs a mechanism to prevent duplication of frames. Generally, error control is obtained via a trailer added to the frame end.

(e) Access Control – Data link layer protocols are required to decide which device has control over the link at any given time if two or more devices are connected to the same link.

(iii) Network Layer – The network layer is responsible for the source to destination delivery of a packet across multiple networks (links).

There is no need for a network layer when two systems are connected to the same link. However, there is a require for network to achieve source to destination delivery when two systems are connected to several networks (link) with connecting devices among the networks (links). Specific functions

of the network layer include the following –

(a) Routing – If independent networks or links are con together to develop an internetwork (a network of networks) or a large net the connecting devices (known as routers or gateways) route the pack their final destination.

(b) Logical Addressing – The addressing problem is h handled by the physical addressing implemented by the data link layer. An addressing system is required to help distinguish the source and destin systems when a packet passes the network boundary. A header is add the network layer to the packet coming from the upper layer that, a other things, includes the logical addresses of the transmitter and receiv

(iv) Transport Layer – For source-to-destination (end-to- delivery of the entire message, the transport layer is responsible. Whi network layer oversees end-to-end delivery of individual packets, it doe recognize any relationship between those packets. In other word, the tran layer, ensures that the entire message arrives intact and in order, overs both flow control and error control at the source-to-destination level. Spe functions of the transport layer include the following –

(a) Segmentation and Reassembly – Message is splitted transmittable segments, every segment having a sequence number. T numbers enable the transport layer for reassembling the message accu upon arriving at the destination and for identifying and replacing packets were lost in the transmission.

(b) Error Control – Similar to the data link layer, the tran layer is responsible for error control. However, at this layer, error cont done end-to-end rather than across a single link. Sending transport layer en that the whole message arrives at the receiving transport layer without Usually, error correction is obtained through retransmission.

(c) Service-point Addressing – Computers often run programs at the same time. Due to this reason, source-to-destination del means delivery not only from one computer to the next but also from a spe process (running program) on one computer to a specific process (ru program) on the other. Therefore, the transport layer header must incl type of address known as a service-point address (or port address). The packet is received by the network layer to the correct computer. The com message is received by the transport layer, to the correct process o computer.

(d) Flow Control – Similar to the data link layer, the tra layer is responsible for flow control. But, at this layer, flow control i end-to-end rather than across a single link.

(e) Connection Control – This layer can be either connection- oriented or connectionless. A connectionless transport layer deals with each segment like an independent packet and delivers it to the transport layer at the destination machine. A connection is established by connection-oriented transport layer with the transport layer at the destination machine first before delivering the packets. The connection is terminated, after all the data are transferred.

(v) Session Layer – The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction between communicating systems. Specific functions of the session layer include the following –

(a) Synchronization – This layer permits a process to add checkpoints (synchronization points) into a data stream. For example, at the time of sending a file of 2000 pages by a system, it is advisable to insert a checkpoint after every 100 pages to make sure that each 100 page unit is received and acknowledged independently.

(b) Dialog Control – This layer permits two systems to enter into a dialog. It permits the communication between two processes to occur either in half-duplex (one way at a time) or full-duplex (two ways at a time).

(vi) Presentation Layer – The function of the presentation layer is to ensure that communicating machines can interoperate properly. For application programs to understand the information transferred between devices which have different internal data representations, a common syntax must be used. This syntax represents information such as character codes, data types, and file formats. Hence, the presentation layer protocols determine what syntax to use when applications in different machines exchange information. Presentation layer has the following specific responsibilities –

(a) Encryption – A system must be able to assure privacy for carrying sensitive information. Encryption means that the transmitter transforms the original information to another form and transmits the resulting message out over the network. The original process is reversed by the decryption to transform the message back to its original form.

(b) Translation – Usually, the processes (running programs) in two systems are exchanging information in the form of character strings, numbers and so on. Before being transmitted, the information should be converted to bit streams. The presentation layer is responsible for interoperability between these different encoding methods because different computers use different encoding systems. At the transmitter, presentation layer converts the information from its sender-dependent format into a common format. At the receiving machine, the presentation layer converts the common format into its receiver-dependent format.

(c) Compression – Data compression minimizes the nu of bits to be sent. Data compression is particularly important in the transm of multimedia such as text, audio and video.

(vii) Application Layer – The application layer enables the us access the network. It gives user interfaces and support for services suc electronic mail, remote file access and transfer, etc. Following specific ser are provided by the application layer –

(a) File Transfer, Access, and Management (FTAM) – application permits a user to access files in a remote computer (to make cha or read data), to retrieve files from a remote computer, and to manag control files in a remote computer.

(b) Network Virtual Terminal – This is a software version physical terminal and permits a user to log on to a remote host. For doing application develops a software emulation of a terminal at the remote host. U computer talks to the software terminal, that in turn, talks to the host, and vice v

(c) Directory Services – Distributed database sources access for global information about different objects and services are prov by this application.

(d) Mail Services – The basis for e-mail forwarding and sto are provided by this application.

Q.28. Write the functions of each layer. ***(R.G.P.V., June***

Ans. Refer the ans. of Q.27.

Q.29. Write functions of data link layer.

(R.G.P.V., June 2010, Dec.

Or

What are the various functions performed by the data link layer

(R.G.P.V., June

Ans. Refer the ans. of Q.27 (ii).

Q.30. What are the services provided by transport layer ?

(R.G.P.V., June

Ans. Refer the ans. of Q.27 (iv).

Q.31. What are the functions of presentation layer ? Justify the need of presentation layer in the architecture of OSI with suitable example.

(R.G.P.V., Dec.

Or

State the major functions performed by the presentation layer in ISO-OSI model.

(R.G.P.V., May

Ans. Refer the ans. of Q.27 (vi).

Q.32. Explain the design issues and functionality of ISO-OSI model. ***(R.G.P.V., Dec. 2017)***

Ans. Refer the ans. of Q.24 and Q.27.

Q.33. Discuss TCP/IP model in detail. ***(R.G.P.V., Dec. 2010)***

Or

Explain in detail TCP/IP reference model. ***(R.G.P.V., June 2013)***

Ans. The ARPANET was a research network sponsored by the DoD (U.S. Department of Defense). It eventually connected hundreds of universities and government installations using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so a new reference architecture was needed. Thus, the ability to connect multiple networks together in a seamless way was one of the major design goals from the very beginning. This architecture later became known as the ***TCP/IP reference model*** after its two primary protocols.

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers – host-to-network, internet, transport and application.

Application Layer
Transport Layer
Internet Layer
Network Access Layer
Physical Layer

Fig. 1.14 The TCP/IP Reference Model

Besides the OSI model another model which is in practical use is the TCP/IP model which is five layer model as shown in fig. 1.14. Internet services generally support TCP/IP protocol. The functions of various layers are discussed below –

(i) Physical Layer – It covers the physical interface between a data transmission device (e.g., workstation, computer) and a transmission medium or network. This layer is concerned with specifying the characteristics of the transmission medium, the nature of the signals, the data rate, and related matters.

(ii) Network Access Layer – The network access layer is concerned with the exchange of data between an end system and the network to which it is attached. The sending computer must provide the network with the address of the destination computer, so that the network may route the data to the appropriate destination. The sending computer may wish to invoke certain services, such as priority that might be provided by the network. The specific software used at this layer depends on the type of network to be used-different standards have been developed for circuit-switching, packet-switching, local area networks and others. This protocol is not defined and varies from host-to-host and network-to-network.

(iii) Internet Layer – All these requirements led to the choice of a packet-switching network based on a connectionless internetwork layer. This

layer, known as internet layer, is the linchpin that holds the whole architec together. The internet layer defines an official packet format and proto called *IP (Internet Protocol)*. The internet protocol is used at this laye provide the routing function across multiple networks. This protoco implemented not only in the end systems but also in the routers. A router processor that connects two networks and whose primary function is to r data from one network to the other on its route from the source to the destina end system.

(iv) Transport Layer – This layer is designed to permit peer entit on the source and destination hosts to carry on a conversation, just as in OSI transport layer. Two end-to-end transport protocols have been defi here. The first one, TCP (Transmission Control Protocol) is a relia connection-oriented protocol that allows a byte stream originating on machine to be delivered without error on any other machine in the Interne fragments the incoming byte stream into discrete messages and passes e one on to the internet layer. TCP also handles flow control to make sure a transmitter cannot swamp a slow receiver with more messages than it handle.

The second protocol in this layer, UDP (User Datagram Protocol) is unreliable connectionless protocol for application that do not want TC sequencing or flow control and wish to provide their own. It is also wid used for one-shot, client-server type request-reply queries and applications which, prompt delivery is more important than accurate delivery such transmitting speech or video.

(v) Application Layer – On top of the transport layer is application layer. It contains all the higher-level protocols. The early o included virtual terminal (TELNET), file transfer (FTP), and electronic m (SMTP). The virtual terminal protocol allows a user on one machine to l onto a distant machine and work there. The file transfer protocol provides way to move data efficiently from one machine to another. Electronic m was originally just a kind of file transfer, but later a specialized protocol (SMT was developed for it. Many other protocols have been added to these over years – the Domain Name System (DNS) for mapping host names onto th network addresses, NNTP, the protocol for moving USENET news artic around, and HTTP.

Q.34. How does the layer of TCP/IP protocol suite correlate to the lay of OSI model ?

(R.G.P.V., Dec. 20

Or

Compare OSI and TCP/IP reference model.

(R.G.P.V., June 2010, Dec. 20

Ans. Since TCP/IP protocol was designed before the OSI model, therefore the layers in TCP/IP do not correspond exactly to the OSI layers. The application layer in TCP/IP is equivalent to the combined session, presentation and application layers of the OSI model. This signifies that all of the functionalities associated with those three layers are handled in one single layer, the application layer as shown in fig. 1.15.

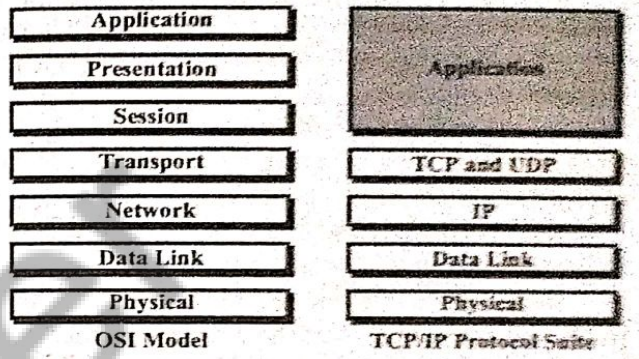


Fig. 1.15 Comparison between OSI and TCP/IP

In other words, every application program must include all tasks assigned to the session, presentation, and application layers of the OSI model. This has one advantage, each application program is independent. It requires only those functions needed for the job for which the application is designed. One disadvantage is that the same tasks appear in different application programs, making them more complex. This damage the whole concept of modularity and layered architecture of the OSI model.

The comparison of the OSI and TCP/IP reference model is as follows –

Similarities –

(i) Both are based on the concept of a stack of independent protocols.

(ii) The functionality of the layers is roughly similar.

For example, in both models, the layers up through and including the transport layer are there to provide an end-to-end network-independent transport service to processes wishing to communicate. These layers form the transport provider. Again in both models, the layers above transport are application-oriented users of the transport services.

Differences –

(i) The OSI model focuses on three concepts –

(a) Services – Each layer performs some services for the layers above it. The service definition tells what the layer does, not how the entities above it access it or how the layer works.

(b) Interfaces – A layer's interface tells the processes above it how to access it. It tells nothing about the layer's internal working.

(c) Protocols – The peer protocols used in a layer carry out all the activities/transactions of the layer. They are internal to the layer and the layer can choose any among the set to carry its business and also change them at will.

The TCP/IP model did not clearly distinguish between services, interfa and protocols. Consequently, the protocols in the OSI model are better hid than in the TCP/IP model and can be replaced relatively easily as the technol changes.

(ii) The OSI reference model was devised before the protoc were invented. This ordering means that the model was not biased towa one particular set of protocols but the problem was that the designer did have much experience with the subject and did not have a good idea of wh functionality to put in which layers.

While in TCP/IP model, the protocols came first, and the model really just a description of the existing protocols. There was no problem the protocols fitting the model. The only trouble was that the model did not any other protocol stacks.

(iii) The two models also differ in the number of layers – the O model has seven layers and the TCP/IP has four layers. Both have netwo transport and application layers, but the other layers are different.

(iv) The OSI model supports both connectionless and connecti oriented communication in the network layer, but only connection-orient communication in the transport layer. The TCP/IP model supports on connectionless communication in the network layer but supports both mod in the transport layer giving the users a choice.

Q.35. Explain the layered architecture of OSI model. List two ways which OSI model and TCP/IP model are same. ***(R.G.P.V., June 20***

Ans. Refer the ans. of Q.27 and Q.34.

Q.36. Write difference between OSI and TCP/IP model. ***(R.G.P.V., June 20***

Ans. Refer the ans. of Q.34.

Q.37. Explain TCP/IP model in brief. Differentiate it with seven layer model. ***(R.G.P.V., June 20***

Ans. Refer the ans. of Q.33 and Q.34.

PRINCIPLES OF PHYSICAL LAYER – MEDIA, BANDWIDTH DATA RATE AND MODULATIONS

Q.38. Give the basic principle of physical layer in brief.

Ans. Physical layer mainly deals with communication between adjac nodes connected via. wired/wireless telecommunication links.

The basic principle of operation of the physical layer is illustrated fig. 1.16.

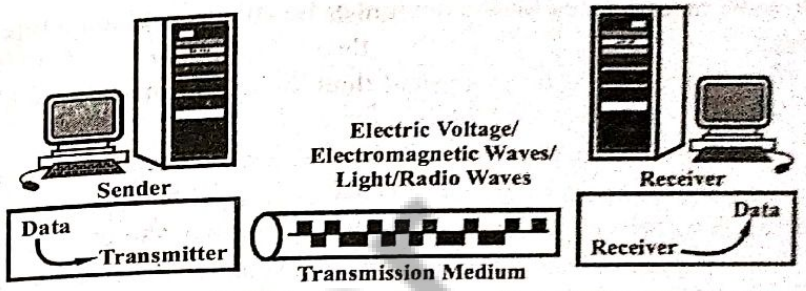


Fig. 1.16 Basic Principle of Operation of Physical Layer

At the sending node physical layer implementation,

(i) Data is treated as a stream of bits.

(ii) The physical layer converts each bit (0 to 1) into an appropriate electrical or optical signal and transmits the signal via wired or wireless telecommunication links. This conversion process is known as ***line encoding***.

(iii) For each bit that is transmitted, the sending node physical layer transmits the corresponding electrical/optical signal for a certain finite duration of time. This duration of time is known as the ***bit interval***.

At the receiving node physical layer implementation,

(i) The incoming signals are first converted back into the corresponding bits. This is known as ***line decoding*** and is usually the reverse process as that of line encoding.

(ii) The bits are then handed to the receiver's data link layer for further processing.

Q.39. What is purpose of physical layer ? Discuss briefly the physical layer protocol.

Ans. Transmission of digital information from one device to another is the basic function for the devices to be able to communicate. The first layer of the OSI model, the physical layer which carries out this function. Relaying through the use of modems is a very important data transmission function carried out at the physical layer level.

Let us consider a simple data communication situation shown in fig. 1.17, where two digital devices A and B need to exchange data bits.

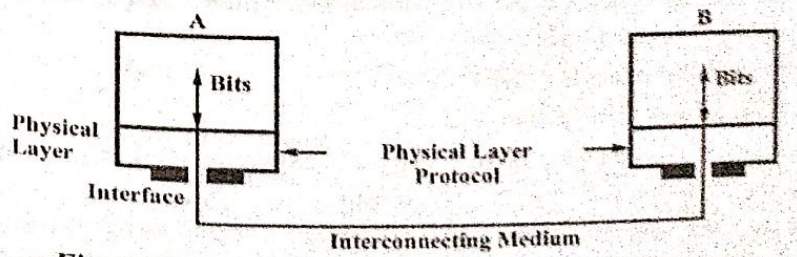


Fig. 1.17 Transmission of Bits by the Physical Layer

The basic requirements for the devices to be able to exchange bits are following –

(i) There should be a physical interconnecting medium which carry electrical signals between the two devices.

(ii) The bits need to be converted into electrical signals and vice

(iii) The electrical signal should have characteristics (voltage, impedance, rise time etc.) suitable for transmission over the medium.

(iv) The devices should be prepared to exchange the electrical

These requirements, which are related purely to the physical aspe transmission of bits, are met out by the physical layer. The rules and proc for interaction between the physical layers are called physical layer pro (fig. 1.17).

The physical layer provides its service to the data link layer which next higher layer and uses this service. It receives service of the p interconnection medium for transmitting the electrical signals.

Q.40. Describe the physical medium interface with related diagr

Ans. The physical layers need to exchange protocol control inform between them. Unlike the other layers which send the protocol c information as a separate field, the physical layers use the intercon medium for sending the protocol control signals. These signals are s separate wires as shown in fig. 1.17. Note that the control signals or and terminate in the physical layers. They have no functional signifi beyond the physical layer. This is in conformity with the principles layered architecture.

The physical interconnecting medium consists of a number of carrying data and control signals. It is essential to specify which wire which signal. Moreover, the mechanical specifications of the connecto of the connector (male or female) and the electrical characteristics signals need to be specified. Definition of the physical medium interface all these specification.

Q.41. What are the types of physical layer media ?

Ans. The three basic types of physical layer media are as follows

(i) Twisted pair wire

(ii) Fibre optic cable

(iii) Wireless technology.

(i) Twisted Pair Wire – The least-expensive and most widel guided transmission medium is twisted pair.

A twisted pair consists of two insulated copper wires arrange regular spiral pattern. A wire pair acts as a single communicati

Typically, a number of these pairs are bundled together into a cable by wrapping them in a tough protective sheath. Over longer distances, cables may contain hundreds of pairs. The twisting tends to decrease the crosstalk interference between adjacent pairs in a cable. Neighbouring pairs in a bundle typically have somewhat different twist lengths to enhance the crosstalk interference. On long distance links, the twist length typically varies from two to six inches. The wires in a pair have thicknesses of from 0.016 to 0.036 inches.

Twisted pair comes in two varieties unshielded and shielded. Unshielded twisted, pair (UTP) is ordinary telephone wire. Office buildings, by universal practice, are pre-wired with a great deal of excess unshielded twisted pair, more than is needed for simple telephone support. This is the least expensive of all the transmission media commonly used for local area networks, and is easy to work with and simple to install.

Unshielded twisted pair is subject to external electromagnetic interference, including interference from nearby twisted pair and from noise generated in the environment. A way to improve the characteristics of this medium is to shield the twisted pair with a metallic braid or sheathing that reduces interference. This shielded twisted pair (STP) provides better performance at lower data rates. However, it is more expensive and more difficult to work with than unshielded twisted pair.

Some advantages of twisted pair wire are as follows –

(a) Twisted pair is most readily installed because it is less rigid than coaxial cable or fiber.

(b) Since wiring ducts suitable for twisted-pair cable are already in place at most office desks for telephony, it is less costly to install additional twisted pairs for data purposes than it is to install new cable ducts for coaxial cable or fiber.

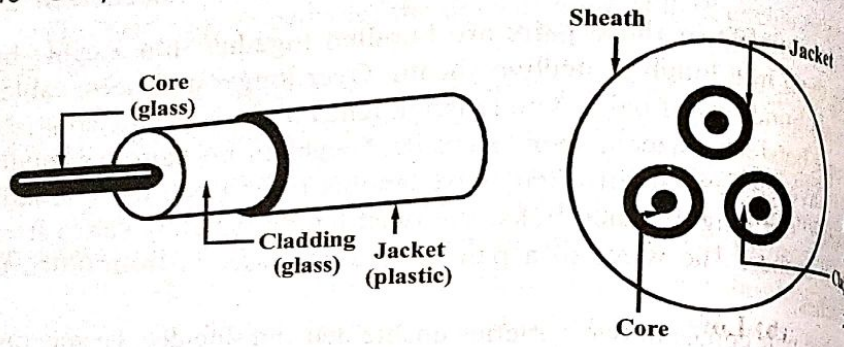
(c) Twisting the wires reduces crosstalk between cable pairs.

(d) Twisting the wires also reduces interference problems.

(e) A twisted pair cable can pass a wide range of frequencies.

(ii) Fibre Optic Cable – Fig. 1.18 (a) shows a single fibre viewed from the side. Fibre optic cables are similar to coax, except without the braid. At the centre is the glass core through which the light travels. In single-mode fibres, core is 8 to 10 microns. In the case of multimode fibres, the core is typically 50 microns in diameter.

To keep all the light in the core, the core is surrounded by a glass cladding with a lower index of refraction than the core. Then, cladding is covered to a thin plastic jacket. Fibres are typically grouped in bundles, protected by an outer sheath. A sheath with three fibres is shown in fig. 1.18 (b).



(a) Side View of a Single Fibre (b) End View of a Sheath with Three

Fig. 1.18

Fibres can be connected in three different methods. First, the terminate in connectors and be plugged into fibre sockets. Connecto about 10 to 20 percent of light. But, they make it easy to reconfigure sy

In the second method, the fibres can be spliced mechanically. Mech splices just lay two carefully cut ends next to each other in a special sleev clamp them in place. Improvement in the alignment can be done by passin through the junction and then making small adjustments to maximize the

In the third method, two pieces of fibre can be fused (melted) to f solid connection. A fusion splice is almost as good as a single drawn fib even here, a small amount of attenuation takes place.

For all three types of splices, reflections can take place at the po splice, and the reflected energy can interfere with the signal.

Two different types of source are used in fibre optic system – the emitting diode (LED) and the injection laser diode (ILD). Both are semicond devices which emit a beam of light when a voltage is given. LED is less operates over a greater temperature range, and has a longer operation The ILD, that operates on the laser principle, is more efficient and can s greater data rates.

(iii) Wireless Technology – Fig. 1.19 shows the commun band for unguided media, ranging from 3 kHz to 900 THz, used for w communication.

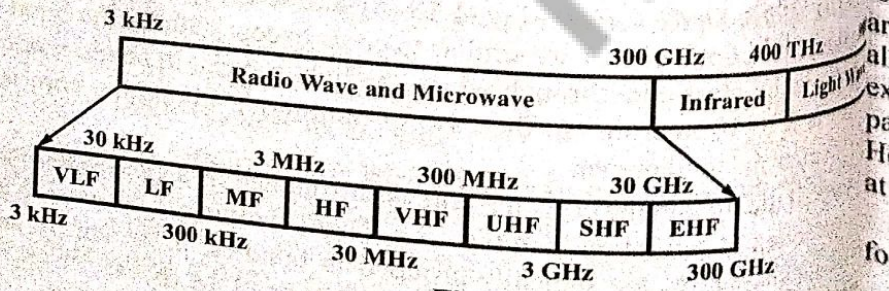


Fig. 1.19

Radio waves and microwaves is divided into eight ranges called bands, each regulated by government authorities. These bands are rated from VLF to EHF.

(a) Very Low Frequency (VLF) – VLF waves propagate as surface waves, usually through air, but sometimes also through water. VLF waves do not suffer attenuation, but atmospheric noise affects them. VLF waves are usually used for long-range radio navigation and submarine communication.

(b) Low Frequency (LF) – LF waves also propagate as surface waves. Attenuation is higher during the daytime. These waves are used for radio beacons and navigation locators.

(c) Middle Frequency (MF) – MF waves rely on line-of-sight antennas to increase and control absorption problems. These waves are used for AM radio.

(d) High Frequency (HF) – HF are used for citizens band ship, international broadcasting, military communiation, telephone, telegraph and facsimile communication.

(e) Very High Frequency (VHF) – VHF waves use line-of-sight propagation and are used for VHF TV, FM radio.

(f) Ultrahigh Frequency (UHF) – UHF waves use line-of-sight propagation. They are used for UHF TV, cellular phones, paging and satellite.

(g) Superhigh Frequency (SHF) – SHF waves are transmitted as either line-of-sight or in the sky. They are used for terrestrial and satellite communication.

(h) Extremely High Frequency (EHF) – EHF waves use line-of-sight propagation and are used for radar and satellite.

Q.42. What are the applications of twisted pair cable ?

Ans. The most common transmission medium for both analog and digital signals is twisted pair. It is the most commonly used medium in the telephone network as well as being the workhorse for communications within buildings.

In the telephone system, individual residential telephone sets are connected to the local telephone exchange or "end office", by twisted pair wire. These are referred to as subscriber loops. Within an office building, each telephone is also connected to a twisted pair, which goes to the in-house private branch exchange (PBX) system or to a centrex facility at the end office. These twisted pair installations were designed to support voice traffic using analog signaling. However, by means of a modem, these facilities can handle digital data traffic at modest data rates.

Twisted pair is also the most common medium used for digital signaling, for connections to a digital data switch or digital PBX within a building, a data

rates of 64 kbps is common. Twisted pair is also commonly used wi building for local area networks supporting personal computers. Data for such products are typically in the neighbourhood of 10 Mbps. Ho recently, twisted pair networks with data rates of 100 Mbps have developed, although these are quite limited in terms of the number of and geographic scope of the network. For long distance applications, t pair can be used at data rates of 4 Mbps or more. Twisted pair is muc expansive than the other commonly used guided transmission media (c cable, optical fibre) and is easier to work with. It is more limited in te data rate and distance.

Q.43. What is the difference between unshielded and shielded t pair cables ?

Ans. Difference between unshielded and shielded twisted Pair cabl as follows –

S.No.	Unshielded Twisted Pair	Shielded Twisted Pair
(i)	Unshielded twisted pair (UTP) cable is composed of a set of twisted pairs with a simple plastic encasement.	Shielded twisted pair (STP) i insulated cable which incl bundled pairs wrapped in t shielding.
(ii)	It suffers more external electro-magnetic interference.	It suffers less external ele magnetic interference becau shielding.
(iii)	It has low capacity in terms of data rate.	It provides better perform at higher data rates.
(iv)	This is least expensive of all trans-mission media and is easy to work with.	This is more expensive than cable and is more difficult to with.
(v)	It is widely used in telephone sys-tems and LANs.	It is used in an electrically environment to limit the e of noise absorptions.

Q.44. What is the effect of cladding in optical fibre cables ?

Ans. Cladding is one or more layers of materials of lower refractive in intimate contact with a core material of higher refractive index. The cl causes light to be confined to the core of the fibre by total internal reflec the boundary between the two. Light propagation in the cladding is supp in typical fibre. The purpose of cladding is to minimise surface losses guide the light waves. The glass used for both the core and the claddin be of very high purity since any impurities present will cause some sca of light to occur. Cladding increases the mechanical strength of the fib also protects the core from absorbing surface contaminants with w could come into contact.

Q.45. Write down the advantages of optical fibre.

Ans. Fibre optic cable has several advantages over metallic cable (twisted pair or coaxial).

(i) Higher bandwidth – Fibre optic cable supports higher bandwidth than either twisted pair or coaxial cable. Currently, data rates and bandwidth utilization over fibre optic cable are limited not by the medium but by the signal generation and reception technology available.

(ii) Less Signal Attenuation – Fibre optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted pair cable.

(iii) Immunity to Electromagnetic Interference – Electromagnetic noise cannot affect fibre optic cables.

(iv) Resistance to Corrosive Materials – Glass is more resistant to corrosive materials than copper.

(v) Light Weight – Fibre optic cables are much lighter than copper cables.

(vi) Greater Immunity to Tapping – Fibre optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Q.46. Write down the disadvantages of optical fibre.

Ans. The main disadvantages of fibre optics are cost, installation/ maintenance, and fragility.

(i) Cost – Fibre-optic cable is expensive. Because any impurities or imperfections in the core can throw off the signal, manufacturing must be painstakingly precise. Also, a laser light source can cost thousands of dollars, compared to hundreds of dollars for electrical signal generators.

(ii) Installation/Maintenance – Any roughness of cracking in the core of an optical cable diffuses light and alters the signal. All splices must be polished and precisely fused. All connections must be perfectly aligned and matched for core size and must provide a completely light-tight seal. Metallic media connections, on the other hand, can be made by cutting and crimping using relatively unsophisticated tools.

(iii) Fragility – Glass fibre is more easily broken than wire, making it less useful for applications where hardware portability is required.

Q.47. Describe briefly about radio waves.

Ans. Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

Radio waves, for the most part are omnidirectional. When an a transmits radio waves, they are propagated in all directions. This mea the sending and receiving antennas do not have to be aligned. A sending a sends waves that can be received by any receiving antenna. The omnidire property has a disadvantage, too. The radio waves transmitted by one a are susceptible to interference by another antenna that may send signal the same frequency or band.

Radio waves, particularly those waves that propagate in the sky can travel long distances. This makes radio waves a good candidate for distance broadcasting such as AM radio.

Radio waves particularly those of low and medium frequencies, can pen walls. This characteristic can be both an advantage and a disadvantage. I advantage because for example, an AM radio can receive signals inside a bui It is a disadvantage because we cannot isolate a communication to just ins outside a building. The radio wave band is relatively narrow just under 1 compared to the microwave band. When this band is divided into subban subbands are also narrow, leading to a low data rate for digital communica

Q.48. Describe briefly about microwaves.

Ans. Electromagnetic waves having frequencies between 1 and 300 are called microwaves.

Microwaves are unidirectional. When an antenna transmits micro waves, they can be narrowly focussed. This means that the sending a receiving antennas need to be aligned. The unidirectional property has an ob advantage. A pair of antennas can be aligned without interfering with a pair of aligned antennas. The following describes some characteristi microwave propagation –

(i) Microwave propagation is line-of-sight. Since the towers the mounted antennas need to be in direct sight of each other, towers are far apart need to be very tall. The curvature of the earth as w other blocking obstacles do not allow two short towers to commu by using microwaves. Repeaters are often needed for long dis communication.

(ii) Very high-frequency microwaves cannot penetrate walls characteristic can be a disadvantage if receivers are inside buildings.

(iii) The microwave band is relatively wide, almost 299 Therefore wider subbands can be assigned and a high data rate is possi

(iv) Use of certain portions of the band requires permission authorities.

Q.49. Describe briefly about infrared rays and its applications.

Ans. Infrared waves, with frequencies from 300 GHz to 40 (wavelengths from 1 mm to 770 nm), can be used for short

communication. Infrared waves, having high frequencies cannot penetrate walls. This advantageous characteristic prevents interference between one system and another, a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we use our infrared remote control, we do not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signal useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications – The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate. The ***Infrared Data Association*** (IrDA) an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs and printers. For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC. The standard originally defined a data rate of 75 Kbps for a distance upto 8 m. The recent standard defines a data rate of 4 Mbps.

Q.50. Define the following –

(i) Bandwidth (ii) Data rate.

Ans. (i) Bandwidth – The ***frequency spectrum*** of a signal is the collection of all the component frequencies it contains and is shown using a frequency domain plot. The ***bandwidth*** of a signal is the width of the frequency spectrum (see fig. 1.20). In other words, bandwidth refers to the range of component frequencies, and frequency spectrum refers to the elements within that range. For calculating the bandwidth, subtract the lowest frequency from the highest frequency of the range.

The ***frequency spectrum*** of a signal is the combination of all sine wave signals that make up that signal.

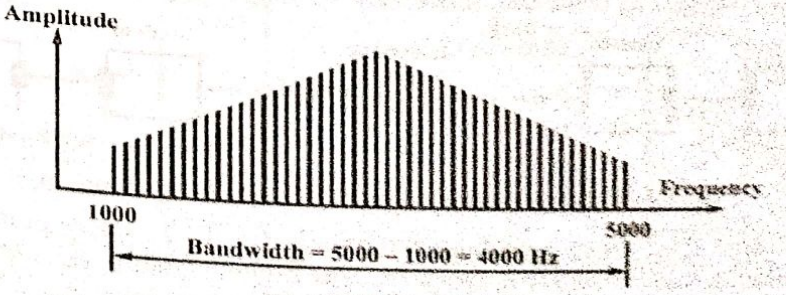


Fig. 1.20 Bandwidth

(ii) Data Rate – The data rate defines the number of data elements (bits) sent in 1s. The unit is bits per second (bps). The data rate is some time

called the bit rate. Increasing the data rate increases the speed of transmissio
The signal rate is the number of signal element sent in 1s. The unit is the ba

Bit rate = Baud rate × No. of bits per signal element.

Q.51. Draw the block diagram of typical modem and explain it.

Ans. The device which performs modulation is called a modulator a
the device which recovers the information signal from the modulated carri
is called a demodulator. In data transmission, we usually come across devic
which perform both modulation as well as demodulation functions and the
devices are called ***modems***. When data is to be transmitted over long distance
modems are needed. In a modem, the input signal modulates a carrier which
transmitted to the distant end. At the distant end, another modem demodulat
the received carrier to obtain the digital signal. Thus, a pair of modems
always required.

The term 'Modem' is derived from the words, MOdulator an
DEModulator. A modem contains a modulator as well as a demodulator. Near
all the modems are designed for utilizing the analog voice band service provide
by the telecommunication network. Thus, the modulated carrier produced b
a modem fits into the 300-400 Hz bandwidth of the speech channel.

Fig. 1.21 shows a typical data connection set up using modems. The digi
terminal devices exchange digital signals and are known as Data Termin
Equipment (DTE). Two modems are always needed, one at each end. At th
transmitting end, the modem converts the digital signal from the DTE into a
analog signal by modulating a carrier. At the receiving end, the modem demodulat
the carrier and hands over the demodulated digital signal to the DTE.

A dedicated leased circuit or a switched telephone circuit can be used
transmission medium between the two modems. In the latter case, modem
are connected to the local telephone exchanges. Whenever data transmissio
is needed, connection between the modems is established through the telephon
exchanges. Modems are also needed within a building to connect termina
which are located at distances, more than 15 metres from the host.

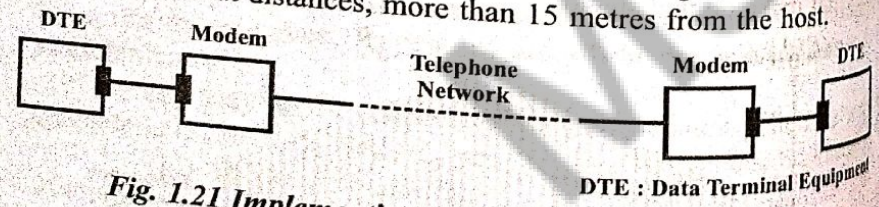


Fig. 1.21 Implementing a Data Circuit Using Modems

A block diagram of a modem is shown in fig. 1.22, which comprises
transmitter, a receiver and two interfaces. The digital signal to be sent is giv
to the transmitter. The modulated carrier that is received from the distant e
is given to the receiver. The digital interface connects the modem to the DT
which produces and receives the digital signals. In order to transmit and receiv
the modulated signals, the line interface connects the modem to the transmissio

channel. Modems connected to telephone exchanges have additional provision
for connecting a telephone instrument, which enables establishment of the
telephone connection.

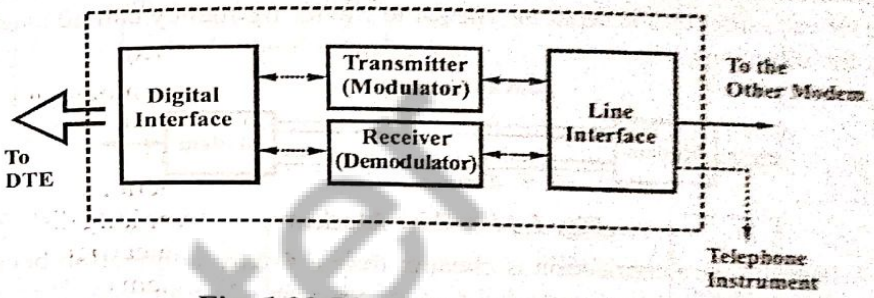


Fig. 1.22 Block Diagram of a Modem

Q.52. Categorizes the modems based on its features.

Ans. Modems can be of several types and they can be categorized in a
number of ways. Categorization is usually based on the following basic modem
features –

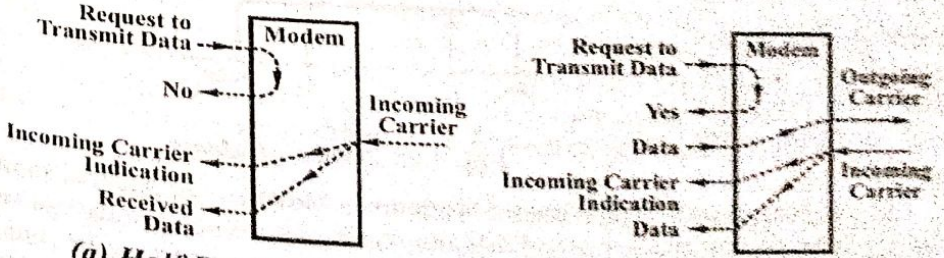
(i) Directional Capability – Half duplex modem and full duplex modem.

(ii) Connection to the Line – 2-wire modem and 4-wire modem.

(iii) Transmission Mode – Asynchronous modem and synchronous
modem.

Half Duplex and Full Duplex Modems – A half duplex modem permits
transmission in one direction at a time. If a carrier is detected on the line by the
modem, it gives an indication of the incoming carrier to the DTE through a
control signal of its digital interface [fig. 1.23 (a)]. So long as the carrier is
being received, the modem does not give clearance to the DTE to transmit.

A full duplex modem allows simultaneous transmission in both directions.
Thus, there are two carriers on the line, one outgoing and the other incoming
[fig. 1.23 (b)].



(a) Half Duplex Modem ***(b) Full Duplex Modem***

Fig. 1.23

2W-4W Modems – The line interface of the modem can have a 2-wire or
4-wire connection to the transmission medium. In a 4-wire connection, one

pair of wires is used for the outgoing carrier and the other is used for the incoming carrier (fig. 1.24). Full duplex and half duplex modes of data transmission are possible on a 4-wire connection. As the physical transmission path for each direction is separate, the same carrier frequency can be used for both the directions.

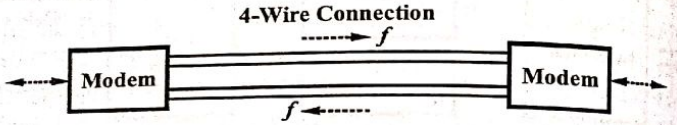


Fig. 1.24 4-Wire Modem

A leased 2-wire connection is cheaper than a 4-wire connection because only one pair of wires is extended to the subscriber's premises. The dial connection established through telephone exchanges is also a 2-wire connection. For the 2-wire connections, modems with a 2-wire line interface are required. Such modems use the same pair of wires for outgoing and incoming carrier.

Half duplex mode of transmission using the same frequency for the incoming and outgoing carriers can be easily implemented [fig. 1.25 (a)]. The transmit and receive carrier frequencies can be the same because only one of them is present on the line at a time.

For full duplex mode of operation on a 2-wire connection, it is necessary to have two transmission channels, one for the transmit direction and the other for the receive direction [fig. 1.25 (b)]. This is achieved by frequency division multiplexing of two different carrier frequencies. These carriers are placed within the bandwidth of the speech channel [fig. 1.25 (c)]. A modem transmits data on one carrier and receives data from the other end on the other carrier.

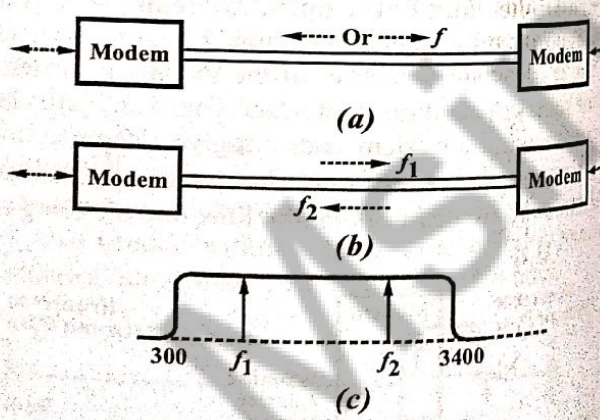
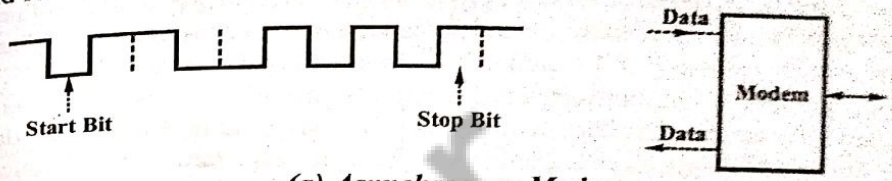


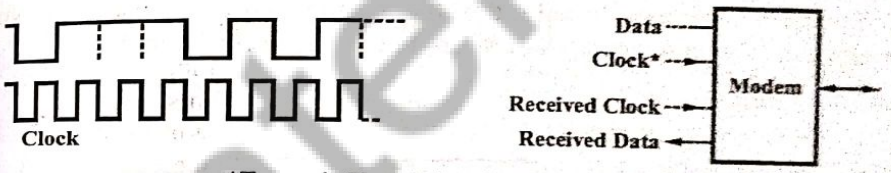
Fig. 1.25 2-wire Modems

Asynchronous and Synchronous Modems – Modems for asynchronous and synchronous transmission are of different types. An asynchronous modem can only handle data bytes with start and stop bits. There is no separate timing signal or clock between the modem and the DTE [fig. 1.26 (a)]. The internal timing pulses are synchronized repeatedly to the leading edge of the start bit.

A synchronous modem can handle a continuous stream of data bits. It requires a clock signal [fig. 1.26 (b)]. The data bits are always synchronized to the clock signal. There are separate clocks for the data bits being transmitted and received.



(a) Asynchronous Modem



*Transmit Clock is Supplied Either by the Modem or by the DTE

(b) Synchronous Modem

Fig. 1.26

For synchronous transmission of data bits, the DTE can use its internal clock and supply the same to the modem. Else, it can take the clock from the modem and send data bits on each occurrence of the clock pulse. At the receiving end, the modem recovers the clock signal from the received data signal and supplies it to the DTE. It is, however, necessary that the received data signal contains enough transitions to ensure that the timing extraction circuit remains in synchronization. High speed modems are provided with scramblers and descramblers for this purpose.

Q.53. What is the function of a "null modem"? Show the internal connections used within a null modem with explanation.

Ans. Suppose you need to connect two DTEs in the same building, for example, two workstations or a terminal to a workstation. Modems are not needed to connect two compatible digital devices directly; the transmission never needs to cross analog lines, such as telephone lines, and therefore does not need to be modulated. But you do need an interface to handle the exchange, just as an EIA-232 DTE-DCE cable does. The solution provided by the EIA standard, is called a ***null modem.*** A null modem provides the DTE-DTE interface without the DCEs.

Many times, it is desirable to connect two terminals over a short distance without using a modem. Essentially, because these terminals are in close proximity of each other, there is no requirement to use telephone lines to interconnect them. In this case, a 'null modem' can be used to do the connection, as shown in fig. 1.27.

In fact, a null modem is an RS-232C cable, which a few wires crossed. Transmit and receive data between both ends are criss-crossed so that the

transmit data of the one terminal is given to the other on the receive da
Data terminal ready (DTR) and data set ready (DSR) lines are also
coupled so that one terminal's DTR output becomes an indication on the
DSR input. Finally, the request-to-send (RTS) output of each terminal is
to its own clear-to-send (CTS) and to the other terminal's carrier-detec
input. A common line between both terminals provides a common
reference for electrical voltages and signals. By using the null-modem
link can be established by two terminals without the requirement for a m
An active RTS from one terminal signals its own CTS and the other ter
CD. Similar action is established at the other terminal and data link is se
the data can flow in serial digital form between the two terminals.

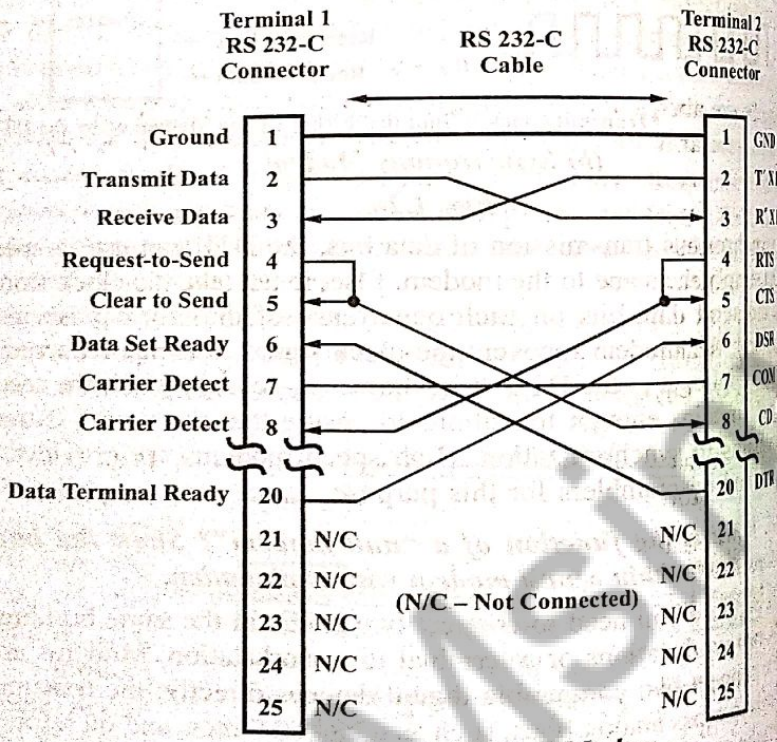


Fig. 1.27 Null Modem

A null modem is an EIA-232 interface that completes the necessary
to fool the DTEs at either end into believing that they have DCEs and a
between them. Since its purpose is to make connections, a null mode
either a length of cable or a device, or we can make one ourself
standard EIA-232 cable and a breakout box which permits us to cross
wires in any way we want. Of these options, the cable is the most c
used and the most convenient.

Q.54. What are fax modems ? Draw and explain the group III transmit and receive block.

Ans. A block diagram for a fax system is shown in fig. 1.28.

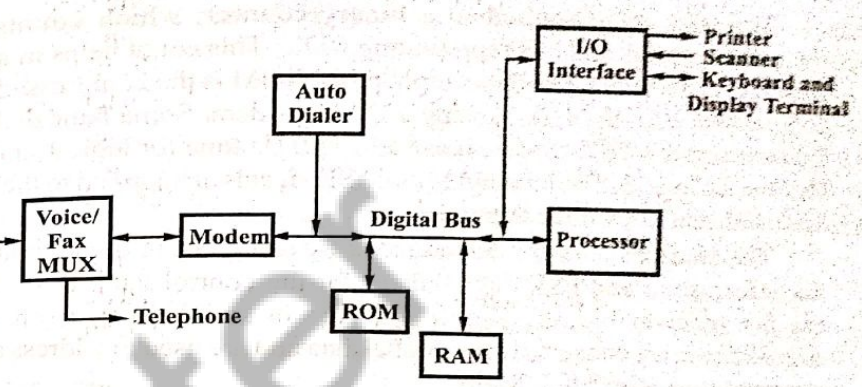


Fig. 1.28 Facsimile System

In the figure above, the Voice/Fax MUX block discerns between a fax bit signal and regular voice call on a telephone line. In this block, voice communications are directed to a telephone handset, while fax data are sent to fax-modem. The fax data are received and demodulates by the modem and are decoded and processed by the processor block. Then it is sent to a specific peripheral, a printer, to produce a hard copy of the document or a terminal for video display. Fax data can be entered into the system through a scanner or from previously scanned data, which is stored on disk or in computer's memory.

The data are encoded and sent to the fax modem for modulation and transmission on the telephone line.

A group III fax transmitter is shown in fig. 1.29. A 1728 bit-per-line digital stream is produced by scanning and sampling of a document.

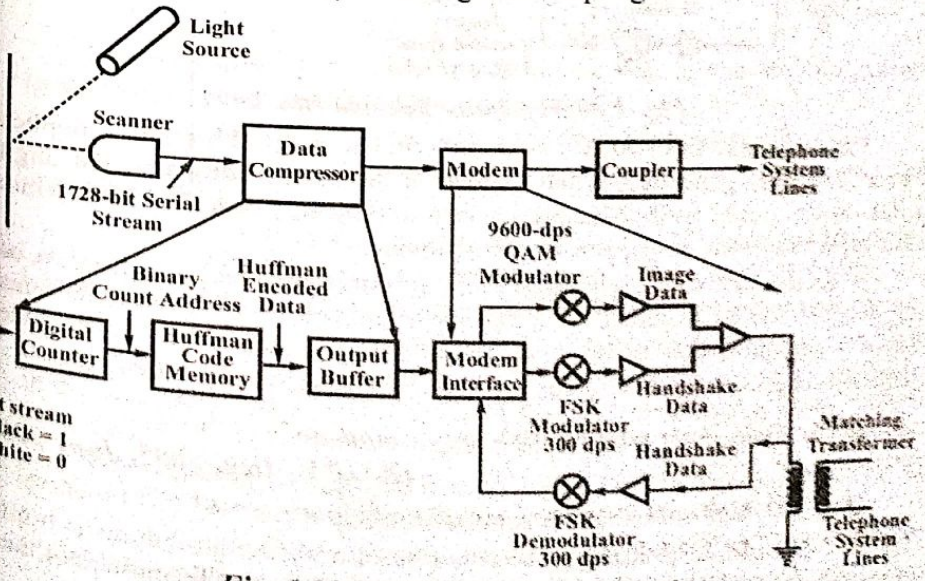


Fig. 1.29 Facsimile Transmit Blocks

This stream is applied to a binary counter, which counts representing black and bits representing white. This count helps in add Huffman code ROM. The data output of the ROM is the compressed H code, which is used in modulating a QAM modem. Some handshake data are sent to a FSK modem using an 1,650 Hz tone for logic 1 and a Hz tone for logic 0. The joint QAM and FSK signals are applied to the te lines and sent to their destination.

The received data are demodulated by using QAM demodulator fax information and FSK demodulator for the control data. Fig. 1.3 the fax receiver blocks. The digital data in serial form, from the demodulator, are converted into parallel data and are used to address a H decompressor (decoder) ROM.

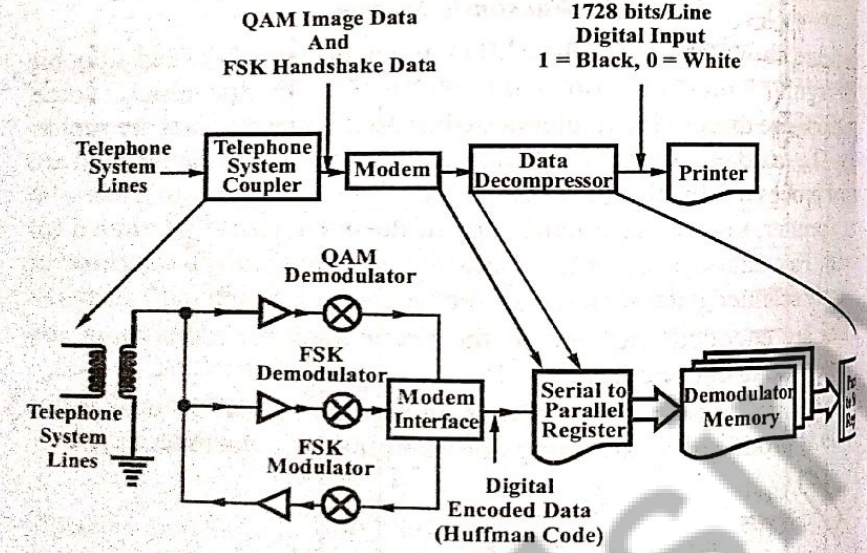


Fig. 1.30 Facsimile Receive Blocks

Parallel data (from ROM) is reconverted to a serial stream to the information generated by the scanner at the transmitting site. This information will be further decoded as required by the printer or video that reproduces the actual document or image.

A fax machine with a sole purpose of transmitting and receiving fax the decoded ROM data directly to reproduce a hard copy of the scanned Some common models of fax modems are – Robotics Sportster FAX (external) with V.42 bis, V.32 bis and V.34 and PCISA internal Modem

Q.55. Write short note on high speed modems.

(R.G.P.V., Dec. 2005, J

Ans. The high speed modems are given below –

(i) 56 K Modems – The data rate of traditional modems to maximum of 33.6 kbps

new modems with a rate of 56,000 bps, known as 56 K modems, are on the market. These modems can be used only when one party is using digital signalling. They are asymmetrical in that the downloading (flow of data from Internet provider to the PC) is a maximum of 56 kbps, while the uploading (flow of data from the PC to the Internet provider) can be maximum of 33.6 kbps. When one side is an Internet provider and the signal does not have to pass through a PCM converter, quantization is eliminated in one direction and the data rate can be increased to 56 kbps, as shown in fig. 1.31.

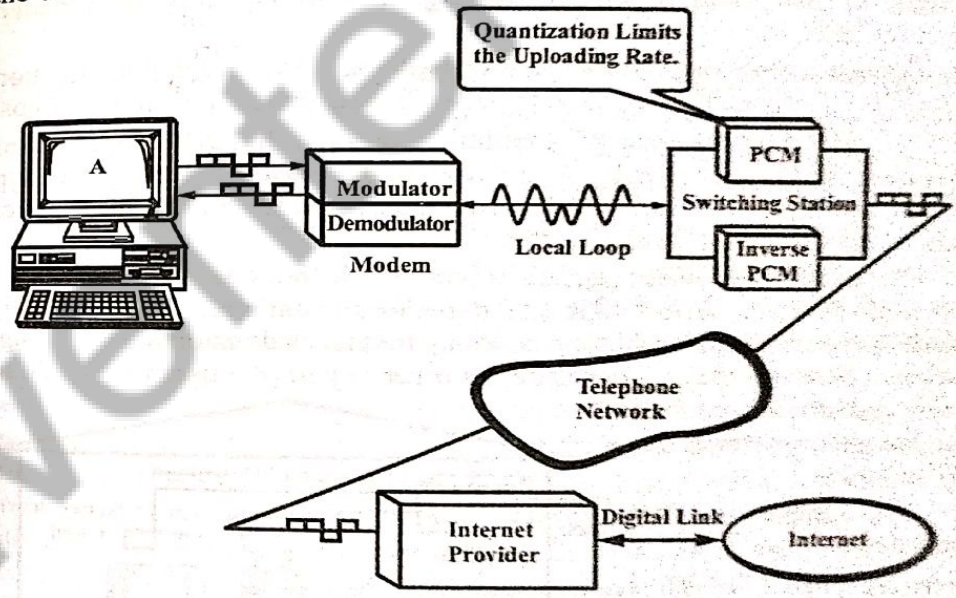


Fig. 1.31 56 K Modems

Transmission of data from the subscriber to the Internet provider ***(uploading)*** occurs in the following steps –

(a) Modem modulates the digital data at site A

(b) Modem transmits the analog data to the switching station at site A on the local loop

(c) Data are converted to digital using PCM at the switching station

(d) Digital data travel through the digital network of the telephone company and are received by the Internet provider computer.

Step (c) is again the limiting factor in these steps, which means there is no improvement here. The user does not require such a high data rate because, in this direction, only small blocks of data (like an e-mail or a small file) are transmitted.

Downloading or transmission of data from the Internet provider to the modem at site A occurs in the following steps –

(a) Computer of the Internet provider transmits the digital data through the digital telephone network

(b) Digital data are converted to analog using inverse PCM the switching station

(c) At site A, the switching station transmits the analog data the modem on the local loop

(d) At site A, analog data are demodulated by the modem.

There is no quantization of data using PCM in this direction. The limitation when uploading is not an issue here; data can be transmitted at 56 kbps. This is what the user is looking for, because large files are typically downloaded from the Internet.

Thus, it is concluded that the maximum data rate in the uploading direction is still 33.6 kbps, but the data rate in the downloading direction is now 56 kbps.

(ii) Cable Modem – The traditional modems have the limitation of data rate, which is mostly due to the narrow bandwidth of the local telephone line (upto 4 kHz). A modem can be designed to handle much higher data rates by using higher bandwidths.

The cable TV provides residential premises with a coaxial cable which has a bandwidth upto 750 MHz and sometimes evenmore. Generally, the bandwidth is divided into 6 MHz bands using frequency division multiplexing and each band provides a TV channel. In order to permit a user to download and upload information from the Internet, two bands can be set aside.

The cable modem concept is shown in fig. 1.32, in which a splitter is used instead of the traditional cable box. The splitter directs the TV bands to the TV set and the Internet access bands to the PC.

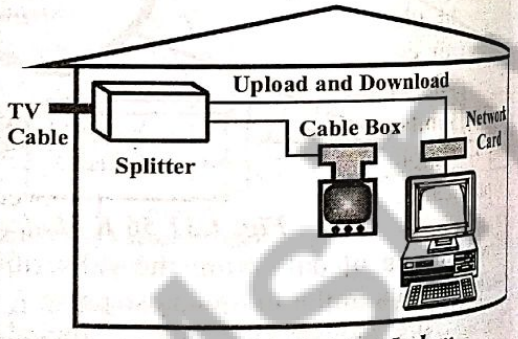


Fig. 1.32 Cable Modem

Downloading, in general, needs a 6 MHz bandwidth in a range above MHz. The 64-QAM technique is used for demodulation. It means that a can download information at a rate of –

$$6 \text{ MHz} \times 6 = 36 \text{ Mbps}$$

But, PCs are not yet capable of receiving data at this rate. Therefore, rate between 3 and 10 Mbps is used presently.

Uploading needs a 6 MHz bandwidth in a range below 40 MHz, as the home appliances can generate a noisy environment which affects modulation. Generally, QPSK technique is used for modulation. It means that a user upload information at a rate of

$$6 \text{ MHz} \times 2 = 12 \text{ Mbps}$$

The uploading rate between 500 kbps and 1 Mbps is used presently.

UNIT 2

DATA LINK LAYER

DATA LINK LAYER – NEED, SERVICES PROVIDED, FRAMING, FLOW CONTROL, ERROR CONTROL

Q.1. What do you understand by data link layer ? Why we need it ?

Ans. Data link layer is the second layer of the open system interconnection (OSI) reference model. The data link layer together with physical layer and the interconnecting medium provide a data link connection for reliable transfer of data bits over an imperfect physical connection. It improves the bit transport service of the physical layer by controlling the errors. The data link layer includes error control, flow control and the associated link management functions. This layer receives the data from the next higher layer and adds some control bits to a block of data bits to transfer to the other devices. The block of data along with the control bits is called frame, which is handed over to the physical layer. The physical layer converts the bits into an electrical signal for transmission over the interconnecting transmission medium. The electrical signal is converted back to bits form by the physical layer at the receiving side and the frame is handed over to the data link layer. The data link layer removes the control bits and checks for errors. It hands over the received data bits to the next layer when no error is found.

The basic service provided by the physical layer is transportation of bits over the physical connection but this capability has certain limitations. If the electrical signal gets impaired due to the noise encountered during transmission or due to the medium characteristics, errors may be introduced in the data bits. There is need to establish mechanisms to control transmission errors. Errors can also be introduced if the receiving device is not ready for the incoming bits and some of the bits are lost. Therefore, a data flow control mechanism also needs to be implemented. The physical layer does not meet these requirements. Error control, flow control and other associated functions are implemented in the data link layer which ensures error free transfer of bits from one device to the other. That's why we need data link layer.

Q.2. State various design issues for data link layer. (R.G.P.V., June

Ans. The design issues for data link layer are discussed below –

(i) Services Provided to the Network Layer – The pri responsibility of data link layer is to provide services to the network layer principle service is transferring data from the network layer on the so machine to the network layer on the destination machine. The two data layers communicate with each other by data link control protocol.

Following are the important services provided by data link layer t network layer –

(a) Unacknowledged Connectionless Service – As the n suggest it is unacknowledged form of transmission. Here, the source mach sends the data to the destination machine without any acknowledgement. this, no connection is either established or released. If the data is lost du noise or interference, the lost data is not even recovered by the layer.

(b) Acknowledged Connectionless Service - acknowledged connectionless service each data frame is acknowledged the destination machine. If any data frame is lost or not arrived in time, same can be transmitted again. In this service no connections are used.

(c) Acknowledged Connection-oriented Service Acknowledged connection-oriented service establishes a connection prior data transmission. Each frame is numbered before transmission a corresponding acknowledgement is also received. The transmission is carr out in distinct phases.

This service provided to be more reliable than other services.

(ii) Framing – To service the network layer, data link layer uses service provided to it by the physical layer. Physical layer accepts the raw stream and delivers it to destination. This bit stream may contain error in number of bits received may not be equal to number of bits transmitted. T data link layer breaks the streams into discrete frames and computes checksum for each frame. At the destination the checksum is recomput The breaking of bit stream by inserting spaces or time gaps is called *frami* Since it is difficult and risky to count on timing and mark the start and end each frame, various simple methods used for framing are –

(a) Character count

(b) Starting and ending characters, with character stuffing

(c) Starting and ending flags, with bit stuffing.

(iii) Error Control – To ensure the proper sequencing and safe deliv of frames at the destination, an acknowledgement should be sent by destination network. The receiver sends back special control frames bear

positive or negative acknowledgements about the incoming frames. If the sender receives a positive acknowledgement it means the frame has arrived safely. A negative acknowledgement means that something has gone wrong and the frame is to be retransmitted. A timer at sender's and receiver's end is introduced. Also sequence numbers to the outgoing frames are maintained so that the receiver can distinguish retransmissions from originals. This is one of the most important part of data link layer duties.

(iv) Flow Control – When the sender is running on fast machine or lightly loaded machine and receiver is on slow or heavily loaded machine, then the transmitter will transmit frames faster than the receiver can accept them. Even if the transmission is error free at a certain point the receiver will simply not be able to handle the frames as they arrive and will start to lose some. To prevent this flow control, mechanism is incorporated which includes a feedback mechanism requesting transmitter a retransmission of incorrect message block. The most common retransmission technique is known as Automatic Repeat Request (ARQ).

Error control in data link layer (DLL) is based on Automatic Repeat Request (ARQ) i.e., retransmission of data in three cases –

(a) Damaged frames (b) Lost frames (c) Lost acknowledgements.

(v) Physical Addressing – If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of sender and/or receiver of the frame.

Q.3. Write a detailed note on framing.

Or

What are the various framing methods ? Explain. (R.G.P.V., June 2012)

Or

How framing is done in data link layer ? Explain. (R.G.P.V., June 2016)

Ans. The data link layer uses the service provided by the physical layer and provides service to the network layer. The physical layer accepts a raw bit stream and attempts to deliver it to the destination. This bit stream is not ensured to be error free. Number of bits received may be less than, equal to, or more than the number of bits transmitted and they may have different values. It is upto the data link layer to detect and, if essential, correct errors.

Generally, the data link layer breaks the bit stream up into discrete frames and computes the checksum for each frame. After arriving a frame at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has happened and takes steps to deal with it.

It is not an easy task to break the bit stream up into frames. One approach to obtain this framing is to insert time gaps between frames, much like the

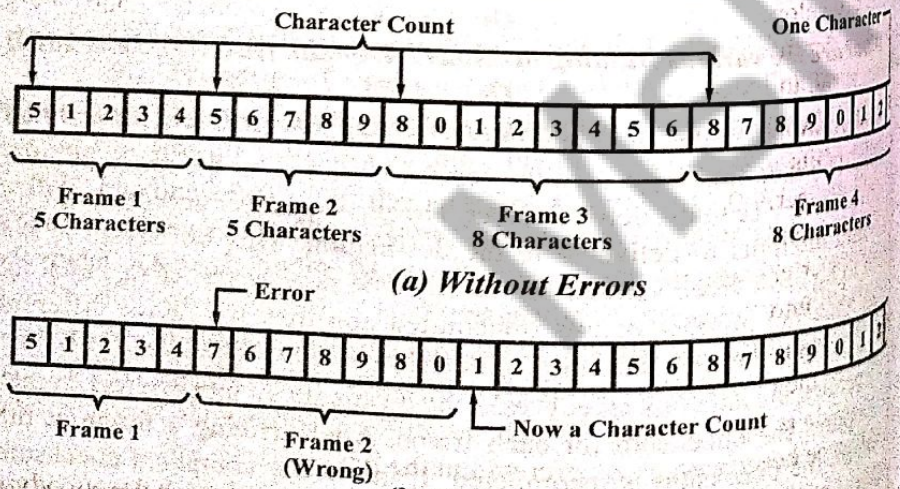
spaces between words in ordinary text. But, the networks rarely make guarantees about timing. Therefore, it is possible these gaps might be squeez out or other gaps might be inserted during transmission.

This is very much risky to count on timing to mark the start and end of a frame. Therefore, other techniques have been devised. There are four techniqu

(i) Character count
(ii) Flag bytes with byte stuffing
(iii) Starting and ending flags, with bit stuffing
(iv) Physical layer coding violations.

In the first framing technique, a field is used in the header to specify number of characters in the frame. By seeing the character count at the destinati data link layer knows how many characters follow and hence where the end the frame is. Fig. 2.1 (a) shows this technique for four frames of sizes 5, 5 and 8 characters respectively. The difficulty with this algorithm is that the co can be garbled by a transmission error. For example, when the character co of 5 in the second frame of fig. 2.1 (b) becomes a 7, the destination will get of synchronization and will be unable to locate the start of the next frame. D to this reason, the character count technique is rarely used anymore.

Second framing technique gets around the problem of resynchronizati after an error by having each frame begin with the ASCII character seque DLE STX and end with the sequence DLE ETX. In this manner, wh destination ever loses track of the frame boundaries, all it has to do is look DLE STX and DLE ETX characters to figure out where it is.


Character Count
One Character
5 1 2 3 4 5 6 7 8 9 8 0 1 2 3 4 5 6 8 7 8 9 0 1 2
Frame 1
5 Characters
Frame 2
5 Characters
Frame 3
8 Characters
Frame 4
8 Characters
Error
5 1 2 3 4 7 6 7 8 9 8 0 1 2 3 4 5 6 8 7 8 9 0 1 2
Frame 1
Frame 2
(Wrong)
Now a Character Count

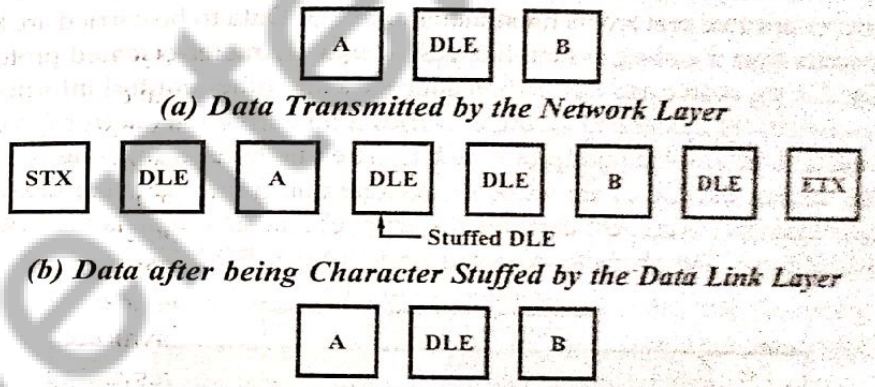
(a) Without Errors

(b) With One Error

Fig. 2.1 Character Stream

This technique has a serious problem when binary data, such as programs of floating-point numbers, are being transmitted. It may easily

that the characters for DLE STX or DLE ETX happen in the data, that will interfere with the framing. One approach to overcome this problem is to have the sender's data link layer insert an ASCII DLE character just before each "accidental" DLE character in the data. At the receiving end, the data link layer removes the DLE before the data are given to the network layer. This technique is known as ***character stuffing.*** Therefore, a framing DLE STX or DLE ETX can be differentiated from one in the data by the absence or presence of a single DLE. DLEs in the data are always doubled. An example data stream before stuffing, after stuffing and after destuffing is shown in fig. 2.2.



(a) Data Transmitted by the Network Layer

(b) Data after being Character Stuffed by the Data Link Layer

(c) Data Passed to the Network Layer on the Receiving Side

Fig. 2.2

This framing method has the disadvantage that it is closely tied to the use of 8-bit characters in general and the ASCII character code in particular. As networks developed, the disadvantage of embedding the character code length in the framing mechanism became more and more obvious. Therefore, a new technique had to be developed to permit arbitrary sized characters.

In the new technique, data frames are permitted to contain an arbitrary number of bits and character codes with an arbitrary number of bits per character are permitted. It works like this. Each frame starts and ends with a special bit pattern, 01111110, known as the ***flag*** byte. Whenever the sender's data link layer encounters five consecutive ones in the data, it automatically stuffs a 0 bit into the outgoing bit stream.

In the bit stuffing, the boundary between two frames can be unambiguously identified by the flag pattern. Therefore, if the receiver loses track of where it is, all it has to do is scan the input for flag sequences, because they can only take place at frame boundaries and never within the data.

Last technique of framing is only useful to networks in which the encoding on the physical medium contains some redundancy. As an example, some LANs encode 1 bit of data by using 2 physical bits. Generally, high-low pair is used for 1, and low-high pair is used for 0. The combinations low-low and

high-high are not used for data. The scheme means that each data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries. This use of invalid physical codes is part of the 802 LAN.

Q.4. What is framing ? Explain different types of framing protocols with their format. ***(R.G.P.V., May 2...)***

Ans. **Framing** – Refer the ans. of Q.3.

Types – The different types of framing protocols are as follows –

(i) Character-oriented Protocols – The format of a frame in character-oriented protocol is illustrated in fig. 2.3. Data to be carried are characters from a coding system like ASCII in a character-oriented protocol. In fig. 2.3, the source and destination addresses and other control information are carried by the header and the trailer carries error correction or error detection redundant bits, are also multiples of 8-bits. The one byte (8-bit) flag is added at the starting and end of the frame to separate one frame from the next. The flag, comprised of protocol-dependent special characters, signals the beginning or end of a frame. The character-oriented protocol is a BISYNC.

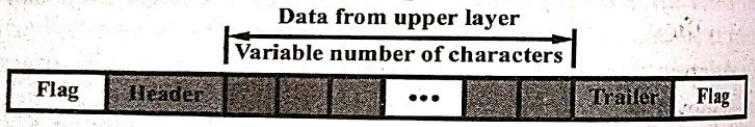


Fig. 2.3

(ii) Bit-oriented Protocols – The data section of a frame is a sequence to be interpreted by the upper layer as text, graphic, audio, video and so on in a bit-oriented protocol. Although, in addition to headers and possible trailers), we still required a delimiter to separate one frame from other. To define the starting and the end of a frame, most protocols employ special 8-bit pattern flag 01111110 as the delimiter, as illustrated in fig. The most popular bit-oriented protocols are SDLC and HDLC.

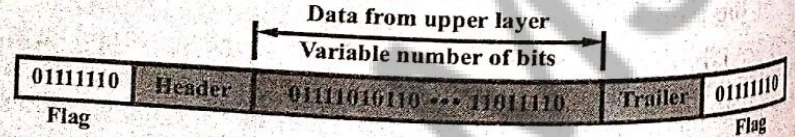


Fig. 2.4

Q.5. What is meant by bit stuffing ? Explain. ***(R.G.P.V., June ...)***

Or

What is the role of bit stuffing in data transmission ?

(R.G.P.V., June ...)

Ans. Bit stuffing is the process of adding one extra 0 bit whenever there are five consecutive 1's in the data so that the receiver does not mistake data for a flag. In data stream, extra bits are inserted to avoid the appearance of unintended control sequences.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs the 0 bit. Just as character (byte) stuffing is completely transparent to the network layer in both computers, so is bit stuffing. If the user data contain the flag pattern, 01111110 this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110. Example of bit stuffing is given below –

(i) 01101111111111111111110010 → Original data

(ii) 0110 11111 011111 0 11111 010010 → Data as they appear on the line

Stuffed bits

(iii) 01101111111111111111110010 → Data as they are stored in the receivers memory after destuffing

Q.6. What is bit stuffing ? If the bit string 0111101111101111110 is subjected to bit stuffing. What is the output string ? ***(R.G.P.V., June 2013)***

Ans. **Bit Stuffing** – Refer the ans. of Q.5.

Given, the input frame is 0111101111101111110. After bit stuffing this input frame is shown as

01111011111001111110 10

Stuffed Bits

Thus, the output frame is 0111101111100111110 10.

Q.7. A bit string, 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing? ***(R.G.P.V., Dec. 2015)***

Ans. Refer the ans. of Q.6.

Q.8. Define data transparency. ***(R.G.P.V., Dec. 2016)***

Ans. With the use of bit stuffing, arbitrary bit patterns can be inserted into the data field of the frame. This property is known as data transparency.

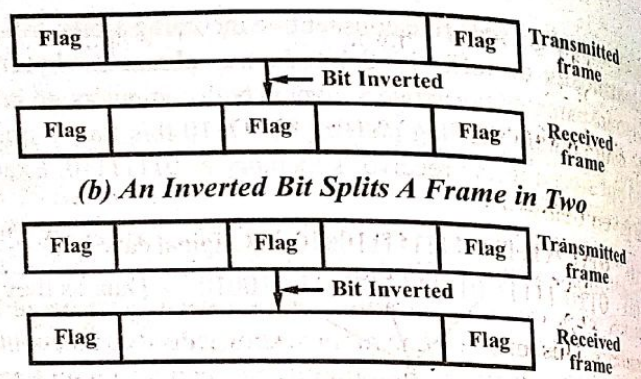
Fig. 2.5 shows an example of bit stuffing. In the first two cases, the extra 0 is not strictly necessary for avoiding a flag pattern but is necessary for the operation of the algorithm. The pitfalls of bit stuffing are also illustrated in this figure. When flag is used as both an ending and a starting flag, a 1-bit error merges two frames into one. Conversely, a 1-bit error inside the frame could split it in two.

Original Pattern – 1 1 1 1 1 1 0 1 1 1 1 1 1 1 0 1 1 1 0 1 1 1 1 1

After Bit Stuffing – 1 1 1 1 1 0 1 0 1 1 1 1 1 0 1 1 0 1 1 1 0 1 1 1 1 1 0

(a) Example

Insventer



(b) An Inverted Bit Splits A Frame in Two

(c) An Inverted Bit Merges Two Frames

Fig. 2.5 Bit Stuffing

Q.9. What is meant by flow control ? How can be achieved flow mechanism ?

Ans. Flow control is a set of procedures which are used to re amount of data, the sender can send before waiting for acknowle The flow of data must not be permitted to overwhelm the receiver. Anyt device contains a limited speed ,at that it can process incoming d receiving device must have the ability to inform the sending devic those limits are reached and to request that the transmitting device fewer frames or stop temporarily. Checking and processing of the i data must be done before they can be used. The rate of such process incoming data is often slower in comparison to the rate of transmiss to this reason, every receiving device has a block of memory, known which is reserved for storing incoming data until they are process the buffer starts to fill up, the receiver must be able to tell the send transmission until it is once again able to receive.

The flow control mechanism can be achieved in the following

(i) When some data is sent, the incoming data has to be and processed at the receiver's side. Since any receiving device has speed of processing and a limited memory to store the data, thus able to tell the transmitting device to send fewer frames or stop until it is once again able to receive. So, the receiver is not overw

(ii) When the frames arrive at the receiver side, acknowledged by sending an ACK frame. If the frame is damaged the receiver sends an error message (NAK frame).

To control the flow of data across communication links, two have been developed –

(i) Stop-and-wait (ii) Sliding window.

Stop-and-wait sends one frame at a time while sliding window sends several frames at a time.

Q.10. Write a short note on error control.

Or

Define error control. ***(R.G.P.V., Dec. 2016)***

Ans. The data link layer gives surity that all frames are eventually delivered to the network layer at the destination and in the proper order. Suppose that, the sender just kept outputting frames without regard to whether they were arriving properly. This might be fine for unacknowledged connectionless service but would most certainly not be fine for reliable, connection-oriented service.

The usual way to ensure reliable delivery is to provide the sender with some feedback about what is happening at the other end of the line. Typically, the protocol calls for the receiver to send back special control frames bearing positive or negative acknowledgements about the incoming frames. It knows the frame has arrived safely when the sender receives a positive acknowledgement about a frame. On the other hand, a negative acknowledgement means that something has gone wrong and the frame must be transmitted again.

Q.11. Name important functions of data link layer. Explain flow control and error control. ***(R.G.P.V., June 2014)***

Ans. **Functions of Data Link Layer** – Refer the ans. of Q.27 (ii) (Unit-I).

Flow Control – Refer the ans. of Q.9.

Error Control – Refer the ans. of Q.10.

DATA LINK LAYER PROTOCOL – ELEMENTARY & SLIDING WINDOW PROTOCOL – 1-BIT, GO-BACK-N, SELECTIVE REPEAT, HYBRID ARQ

Q.12. What is data link protocol ?

Ans. It is necessary that the structure of the frame is known to both the data link layers so that control bits can be recognized. Data link layers should also agree on the set of procedures to be adopted for exchange of control information. Specified set of rules and procedures for carrying out data link control functions is known as ***data link control.***

A data link control specifies the following –

(i) Format of the frame, that is, locations and sizes of the various fields

(ii) Contents of these fields

(iii) Sequence of messages to be exchanged to carry out the flow control, error control and link management functions.

Various manufacturers and organizations develop many data link pro
All these protocols broadly satisfy basic functional needs of the data lin
but services offered are different. Frame formats and contents of
fields are very specific to each protocol. Some examples of data link pro
are as follows –

(i) High-level data link control (HDLC)
(ii) Synchronous data link control (SDLC)
(iii) Advanced data communication control procedure (ADC
(iv) Binary synchronous data link control (BISYNC, BSC).

Q.13. Data link protocols almost always put the CRC in a trailer than in header. Why ? ***(R.G.P.V., June 2006,***

Ans. Data link layer protocols almost always put the cyclic redu
check (CRC) in a trailer rather than in a header because in data link laye
control is normally achieved through a trailer added to the end of the

Also, CRC technique appends the CRC bits to the end of data stre
then the resultant data is sent to the CRC checker for error detection. I
checker the data bits plus CRC bits.are divided by the predetermined
and if the division results in all remainder bits zeros then data is error f
accepted else it is rejected.

The CRC is computed during transmission and appended to the
stream as soon as the last bit goes out onto the wire. If the CRC were
header, it would be necessary to make a pass over the frame to comp
CRC before transmitting. This would require each byte to be handled
once for checksumming and once for transmitting. Using the trailer
work in half.

Q.14. What is piggybacking ? ***(R.G.P.V., June 2009, 201***

Ans. The technique of temporarily delaying outgoing acknowledg
so that they can be hooked onto the next outgoing data frame is k
piggybacking. It is used in the two way transmission of data frames
the communicating stations, in order to improve the use of channel ban

For two stations to exchange data, each station needs to main
windows. One window is required for transit and one for receive.
data and acknowledgements to the other side. Piggybacking provides
support to this requirement. Each data frame includes two fields, one
the sequence number of the frame and another to hold the sequence
of the acknowledgement. Thus, the station sends the data
acknowledgement, together in one frame, saving communication cap
some conditions, if the station has no data to send but to
acknowledgement, then it sends a separate acknowledgement frame

RR (Receive Ready) or RNR (Receive Not Ready). Since the data frame includes a field for acknowledgement, it is necessary to put some value in it, even if there is no new acknowledgement. In such a case, the sequence number of lost acknowledgement is repeated, which the other station ignores being a duplicate one.

Q.15. Discuss about stop-and-wait protocol. ***(R.G.P.V., June 2004, Dec. 2010)***

Ans. In stop-and-wait protocol for flow control, the sender waits for an acknowledgement after every frame it sends. The next frame is sent only after receiving the acknowledgement of previous frame. This process of alternately sending and waiting repeats until the sender transmits an end of transmission frame (see fig. 2.6).

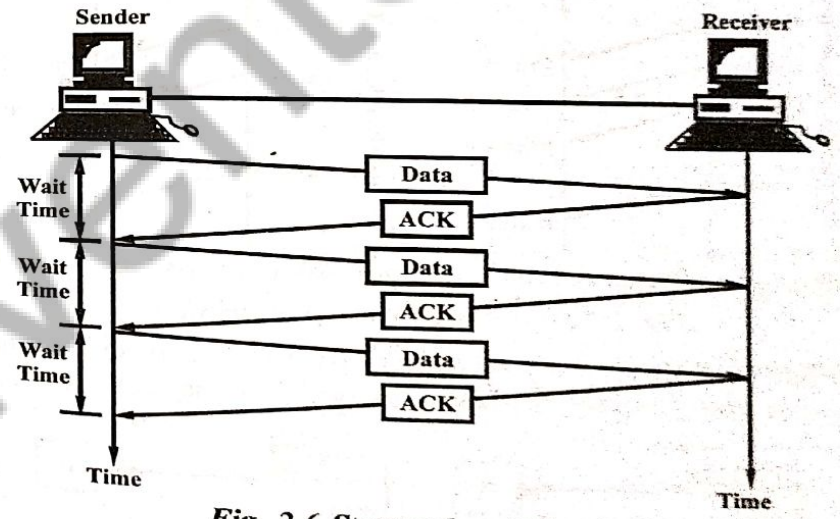


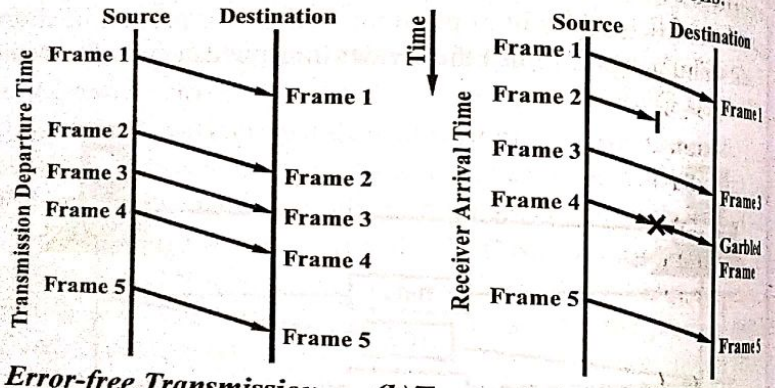
Fig. 2.6 Stop-and-wait Protocol

Stop-and-wait flow control is the simplest form of flow control which works as follows –

A frame is transmitted by a source entity. After the destination entity receives the frame, it shows its desire to accept another frame by sending back an acknowledgement to the frame just received. Before sending the next frame, source must wait until it receives the acknowledgement. Therefore, by withholding acknowledgement, the destination can stop the flow of data. This procedure performs fine and, infact, can hardly be improved upon when a message is sent in a few large frames. However, it is, often the case when a source will break up a large block of data into smaller blocks and sends the data in many frames.

The stop-and-wait procedure may be inadequate with the use of multiple frames for a single message. Serious inefficiencies result in situations where the bit length of the link is greater than the frame length. This is shown in fig.

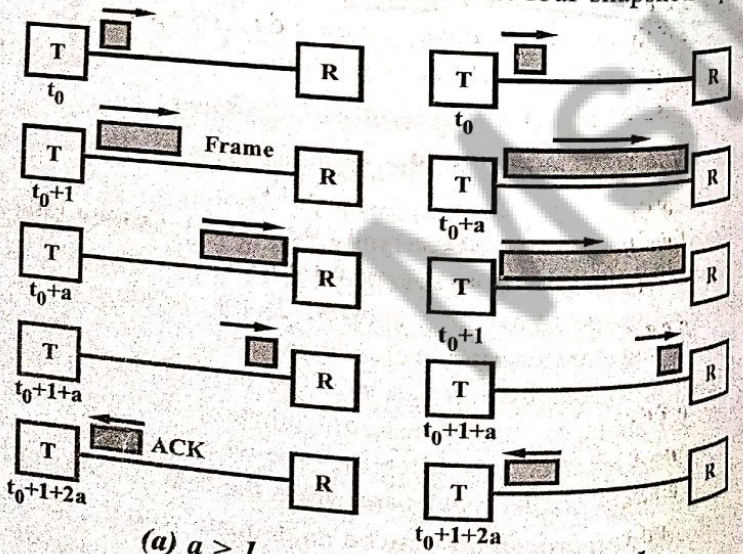
2.7. In this figure, the transmission time is normalized to one and propa
delay is expressed as the variable a. Therefore if a < 1, the propagation
less than the transmission time. In this case, frame is long enough that
bits of the frame have reached at the destination before the co
transmission of the frame by the source. If a > 1, then the propagation
greater than the transmission time. In this case, sender complet
transmission of the whole frame before the leading bits of that frame re
the receiver. This can be said in another way that larger values of a are co
with higher data rates and/or longer distances between stations.



(a) Error-free Transmission *(b) Transmission with Losses and E*

Fig. 2.7 Model of Frame Transmission

Both parts of fig. 2.8 have a sequence of snapshots of the transm
process over time. For both the cases, the first four snapshots repres



(a) a > 1 *(b) a < 1*

Fig. 2.8 Stop-and-wait Link Utilization

process of transmitting a frame containing data and the last snapshot represents the return of a small acknowledgement frame. It should be noted that for a > 1, line is always underutilized and even for a < 1, the line is inefficiently utilized. In the case of very high data rates and very long distances between sender and receiver, stop-and-wait flow control gives inefficient line utilization.

Q.16. What are the reasons for breaking a long data transmission up into a number of frames ? ***(R.G.P.V., Dec. 2016)***

Ans. There are following reasons for breaking a long data transmission upto a number of frames –

(i) The buffer size of the receiver is limited.

(ii) On a shared medium, like LAN, it is normally desirable not to allow one station to occupy the medium for an extended period, therefore causing long delays at the other transmitting stations.

(iii) The longer the transmission, the more likely that there will be an error, necessitating retransmission of the entire frame. Errors can be detected sooner with smaller frames and a smaller amount of data requires to be retransmitted.

Q.17. Write the advantage and disadvantage of stop-and-wait protocol.

Ans. The advantage of stop-and-wait is its simplicity, each frame is checked and acknowledged before the next frame is sent.

The disadvantage is inefficiency; stop-and-wait is slow. Only a single frame uses the entire link from the time it is sent till its acknowledgement is received. Thus if the distance between the sender and the receiver is long, the time spent waiting for ACKs between each frame can be significant portion of the total transmission time.

Q.18. Define propagation delay.

Ans. The propagation delay or t_{prop} is the time required to transmit a packet along the link connecting the source and the destination. This time depends on the type of transmission medium used.

Q.19. Explain stop-and-wait protocol. Derive the expression for utilization. ***(R.G.P.V., June 2014)***

Ans. **Stop-and-wait Protocol** – Refer the ans. of Q.15.

Utilization or Efficiency – It is assumed that a long message is to be transmitted as a sequence of frames F_1, F_2, ..., F_n in the following manners –

(i) Station S_1 transmits F_1

(ii) Station S_2 transmits an acknowledgement

(iii) Station S_1 transmits F_2

(iv) Station S_2 transmits an acknowledgement

.....

(v) Station S_1 transmits F_n

(vi) Station S_2 transmits an acknowledgement.

The total time to transmit the data, T, can be written as $T = nT_F$ T_F is the time to transmit one frame and obtains an acknowledgement. T_F be written as follows –

$$T_F = t_{prop} + t_{frame} + t_{proc} + t_{prop} + t_{ack} + t_{proc}$$

where, t_{prop} is the propagation time from S_1 to S_2, t_{frame} is the time to a frame (time for the transmitter to send out all of the bits of the frame), the processing time at every station to react to an incoming event and the time to transmit an acknowledgement.

Consider the processing time is relatively negligible and the acknowledgement frame is very small in the comparison of a data frame of that are reasonable assumptions. The total time to transmit the data can be expressed as –

$$T = n\,(2t_{prop} + t_{frame})$$

In this time, only $n \times t_{frame}$ is actually spent in transmitting data and rest is overhead. Hence, the utilization or efficiency can be written as-

$$u = \frac{n \times t_{frame}}{n\,(2t_{prop} + t_{frame})} = \frac{t_{frame}}{2t_{prop} + t_{frame}}$$

If the parameter a is defined as –

$$a = \frac{\text{Propagation time}}{\text{Frame transmission time}} = \frac{t_{prop}}{t_{frame}}$$

then,

$$u = \frac{1}{1+2a}$$

This is the maximum possible utilization of the link. Actual utilization lower since the frame has overhead bits. When both t_{prop} and t_{frame} constants, then parameter a is also a constant. This is typically the case fixed-length frames are often used for all except the last frame in a sequence and for point-to-point links, propagation delay is constant.

Q.20. Explain sliding-window protocol in detail.

(R.G.P.V., May/June 2006, June 2012)

Or

What is the mechanism of sliding window flow control ? Explain example.

(R.G.P.V., May

Ans. In stop-and-wait flow control, only one frame at a time can transit. But when the bit length of the link is greater than the frame ($a > 1$), it results serious inefficiencies. By permitting multiple frames to transit at the same time, efficiency can be greatly improved.

Now, we see its working. For this, it is assumed that two stations, A and B, are connected by a full-duplex link. For W frames, station B allocates buffer space. Therefore, B can take W frames and A is permitted to transmit W frames without waiting for any acknowledgement. To keep track of that frames have been acknowledged, a sequence number is labeled for each. By sending an acknowledgement, B acknowledges a frame which includes the sequence number of the next frame accepted. This acknowledgement also implicitly announces that B is made ready to receive the next W frames, starting with the number specified. This method can also be used for acknowledging multiple frames. A maintains a list of sequence numbers which is permitted to send and B maintains a list of sequence numbers which is made to receive. Every list can be thought of as a window of frames. The operation is known as ***sliding-window flow control.***

Sliding-window process is shown in fig. 2.9. In this figure, a 3-bit sequence number is used, so that frames are numbered sequentially from 0 through 7 and then the same numbers are reused for subsequent frames. The shaded rectangle shows the frames which may be sent. In this figure, the sender may transmit five frames, starting with frame 0. Each time a frame is transmitted, the shaded window shrinks. Each time an acknowledgement is obtained, the shaded window increases. Frames between the vertical bar and the shaded-window have been transmitted but not acknowledged. The sender must buffer these frames in case they require to be retransmitted.

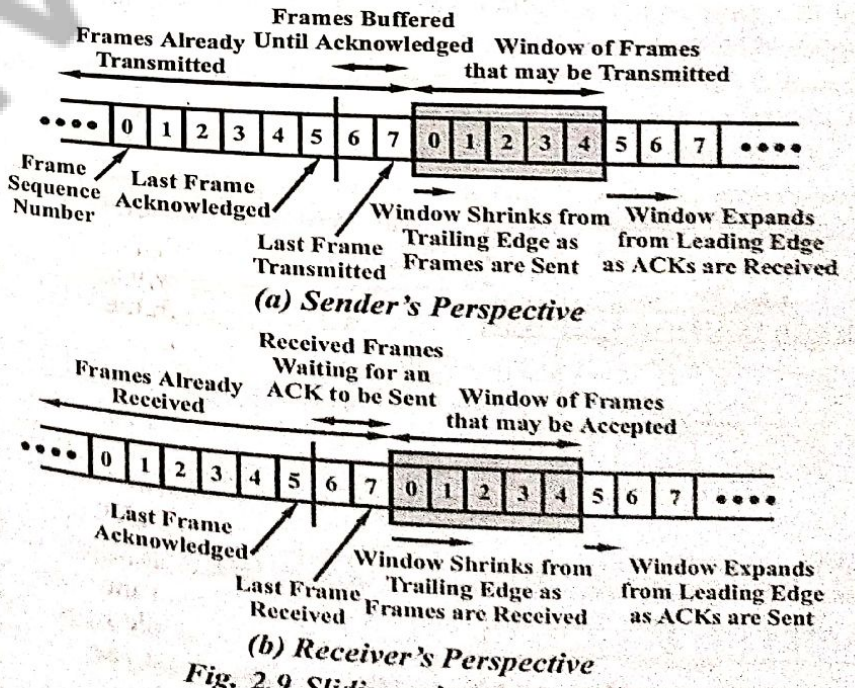

Frames Buffered
Frames Already Transmitted
Until Acknowledged
Window of Frames that may be Transmitted
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
Frame Sequence Number
Last Frame Acknowledged
Last Frame Transmitted
Window Shrinks from Trailing Edge as Frames are Sent
Window Expands from Leading Edge as ACKs are Received
(a) Sender's Perspective
Received Frames
Frames Already Received
Waiting for an ACK to be Sent
Window of Frames that may be Accepted
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
Last Frame Acknowledged
Last Frame Received
Window Shrinks from Trailing Edge as Frames are Received
Window Expands from Leading Edge as ACKs are Sent
(b) Receiver's Perspective

Fig. 2.9 Sliding-window Depiction

Actual window size requires not be the maximum possible size given sequence number length. As example, using a 3-bit sequence num window size of 4 could be configured for the stations using the sliding-w flow control protocol.

Fig. 2.10 shows another example. A 3-bit sequence number field maximum window size of seven frames are assumed in this example. In st A and B have windows showing that A may transmit seven frames, beg with frame 0 (F0). After sending three frames (F0, F1, F2) wi acknowledgement, A has shrunk its window to four frames and a copy of transmitted frames are maintained by it. Window shows that A may tra four frames, starting with frame number 3. Then B sends an RR (receive 3, that means "All frames up through frame number 2 have been received and I am ready to receive frame number 3; in fact, I am ready to receive frames, starting with frame number 3". With this acknowledgement, A is up to permission to send seven frames, still starting with frame 3. A may discard frames which now been acknowledged. A proceeds for transm frames 3,4,5 and 6. B returns RR4 that acknowledges F3 and permits transm of F4 through the next instance of F2. By the time this RR reaches A, already transmitted F4, F5 and F6, and thus A may only open its windo allow sending four frames starting with F7.

Sliding-window flow control is potentially much more efficie comparison to stop-and-wait flow control. The reason behind it is that sliding-window flow control, the transmission link is behaved like a pi which may be filled with frames in transit. On the other hand, only one may be in the pipe at a time.

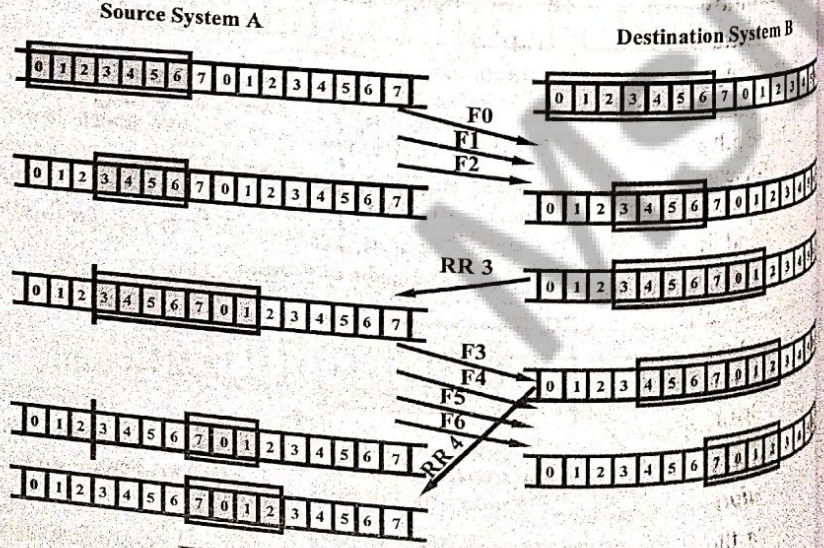


Fig. 2.10 Example of Sliding-window Protocol

Q.21. Explain different flow control mechanisms used in brief. ***(R.G.P.V., May 2019)***

Ans. Refer the ans. of Q.15 and Q.20.

Q.22. How does sliding window protocol help to reduce congestion to an extent ? ***(R.G.P.V., Dec. 2017)***

Ans. In sliding window method of flow control, several frames can be in transmit at a time. Data traffic in full duplex A and B both send the data at the same time so ack signal is send together with data, thus acknowledged signal is called pigged backed.

If A send data to B and then wait for ack. Now if B does not have any data to send it wait for some time for data, if it does not have data than it sends simple ack signal.

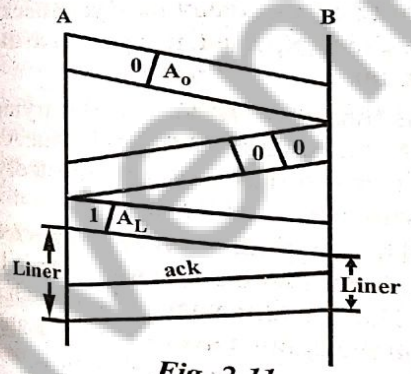


Fig. 2.11

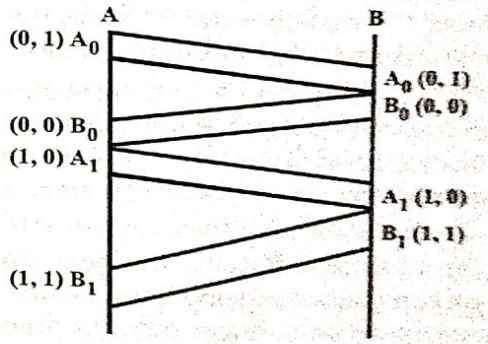


Fig. 2.12

Sliding window protocol has following assumptions –

(i) Data transfer is duplex and concept of piggy tracking is used

(ii) Channel is noisy

(iii) Both sender and receiver have one buffer each

(iv) Receiver has finite processing speed if both station send frame simultaneously.

If both A and B send data simultaneously then each frame send 2 times. So efficiency is decreased to 50%. If there is no error.

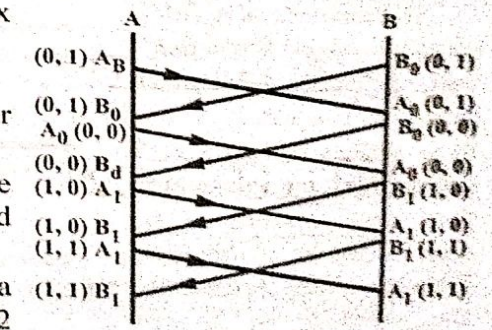


Fig. 2.13

Q.23. Explain sliding window protocol. Also explain how does it help to reduce congestion. ***(R.G.P.V., June 2014)***

Ans. Refer the ans. of Q.20 and Q.22.

Q.24. With the neat sketch explain how each frame will be transmitted twice in one bit sliding window protocol if both end start transmitting simultaneously. ***(R.G.P.V., Dec.***

Or

Write the procedure of one-bit sliding window protocol. ***(R.G.P.V., Nov./Dec.***

Or

Explain 1-bit sliding window protocol. ***(R.G.P.V., Dec.***

Ans. A one-bit sliding window protocol is a bidirectional protocol. In bit sliding window protocol, one of the two data link layers goes first and transmits the first frame. In the event that both data link layers start simultaneously a peculiar situation arises. The starting machine fetches first packet from its network layer, builds a frame from it and transmits this frames arrives, the receiving data link layer checks data link layer to see if it is a duplicate. When the frame is the one expected, it is passed network layer and receiver's window is slid up.

Let us consider A is trying to transmit its frame 0 to B and that B is to transmit its frame 0 to A. Assume that A transmits a frame to B, but timeout interval is a little too short. Consequently, A may time out repeat transmitting a series of similar frames, all with ***seq*** = 0 and ***ack*** = 1.

If the first valid frame arrives at B, it will be accepted, and *frame-exp* will be set to 1. Because B is now expecting frames with sequence numb not 0, all the subsequent frames will be rejected. In addition, B will not new packet from its network layer because all the duplicates have *ack* = B is still waiting for an acknowledgement of 0.

B transmits A a frame containing ***seq*** = 0 and ***ack*** = 0 after every rejected duplicate comes in. Eventually, one of these arrives correctly at A, causing A to start transmitting the next packet. No combination of lost frames or premature timeouts can cause the protocol to deliver duplicate packets to either network layer, or to skip a packet, or to get into a deadlock.

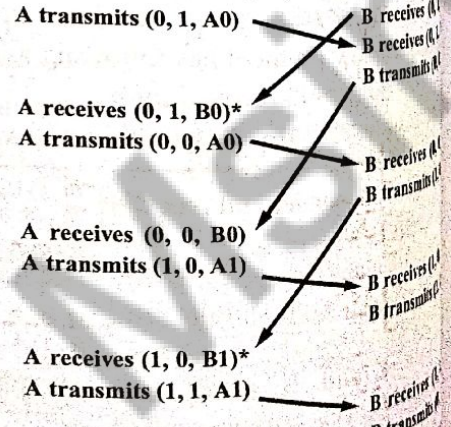


Fig. 2.14 A Scenario for One bit Protocol When both Sides Simultaneously Initiate Communication

If A and B simultaneously initiate communication, their first frames and the data link layers then get into situation shown in fig. 2.14.

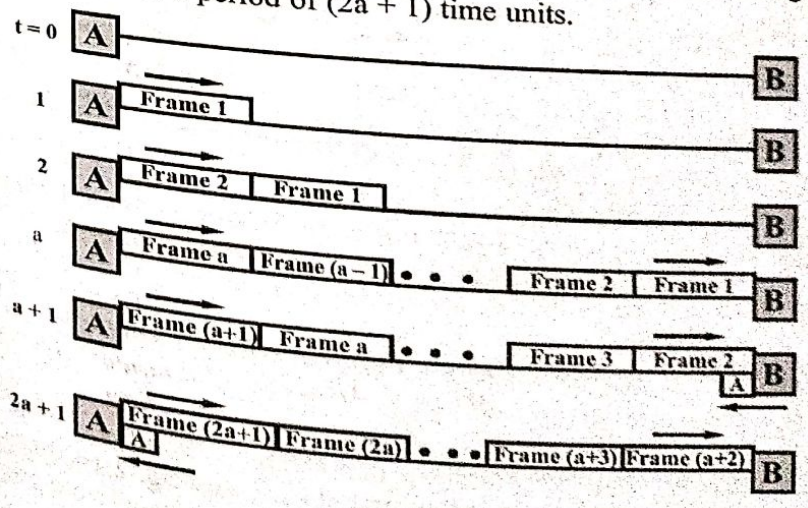
In the fig. 2.14, half of the frames contain duplicates, even though there are no transmission errors. Similar situations can take place as a result of premature timeouts, even when one side clearly starts first. In fact, frames may be sent 3 or more times when multiple premature timeouts take place. Here, the notation is (seq, ack, packet number). An asterisk indicates where a network layer accepts a packet.

Q.25. What is the efficiency of a sliding-window protocol ? ***(R.G.P.V., June 2009)***

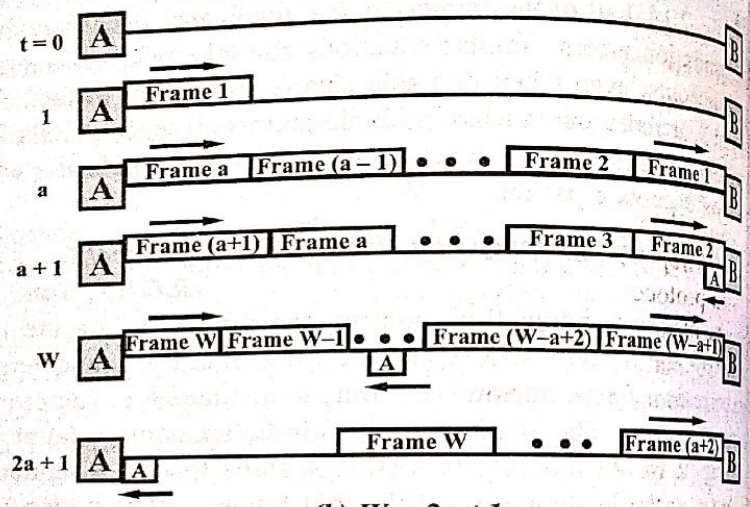
Ans. In sliding-window flow control, the throughput on the line is determined by the window size W and the value of a. For convenience, let us again normalize frame transmission time to a value of 1. Therefore, the propagation time is a. The efficiency of a full-duplex point-to-point line is shown in fig. 2.15. At time t = 0, station A starts to emit a sequence of frames. At t = a, the leading edge of the first frame reaches station B. The first frame is fully absorbed by t = a + 1. If it is assumed that processing time is negligible, B can immediately acknowledge the first frame. Consider the acknowledgement frame be so small that transmission line be negligible. Then, at t = 2a + 1, ACK reaches A. For evaluating performance, two cases are needed to consider –

Case (i) – W ≥ 2a +1. Before A has exhausted its window, the acknowledgement for frame 1 reaches A. Therefore, A can transmit continuously with no pause and normalized throughput is 1.0.

Case (ii) – W < 2a + 1. At t = W, A exhausts its window and cannot transmit additional frames until t = 2a + 1. Therefore, normalized throughput is W time units out of a period of (2a + 1) time units.



(a) W ≥ 2a +1



(b) W < 2a +1

Fig. 2.15 Timing of Sliding-window Protocol

Thus, the utilization can be written as –

$$u = \begin{cases} 1, & W \geq 2a+1 \\ \dfrac{W}{2a+1}, & W < 2a+1 \end{cases}$$

Typically, the sequence number is given for in an n-bit field and $W = 2^n - 1$ is the maximum window size. The maximum utilization achievable for window sizes of 1, 7 and 127 as a function of 'a' is shown in fig. 2.16. Window size of 1 shows the stop-and-wait flow control. Window size of 7 (3 bits) is sufficient for several applications. Window size of 127 (7 bits) is adequate for larger values of a, such as may be obtained in high-speed WANs.

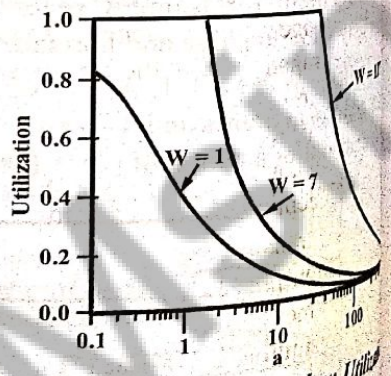


Fig. 2.16 Sliding-window Utilization as a Function of 'a'

Q.26. What is an ARQ ? Explain different ARQ techniques. ***(R.G.P.V., June 2010, Dec.***

Or

Write the different types of ARQ techniques. ***(R.G.P.V., May***

Ans. In the data link layer, error correction is implemented through combined application of an error-detection mechanism, an acknowledgement (ACK) showing successful receipt of a frame, a negative acknowledgement (NAK) showing unsuccessful receipt of a frame, and the specification of which frames are in error. These mechanisms are collectively known as ***Automatic Repeat Request (ARQ).*** There are three ARQ techniques –

(i) Stop-and-wait ARQ

(ii) Go-back-N ARQ

(iii) Selective-repeat ARQ.

(i) Stop-and-wait ARQ – Stop-and-wait ARQ is the simplest transmission protocol. Fundamentally, it uses the stop-and-wait flow control method, but with an additional capability to retransmit lost or corrupted frames. With this additional feature, the receiver discovers an error in a data frame and returns a NAK to the sender showing that the frame should be retransmitted. Thus, source sends out one frame and then waits until it receives either an ACK or a NAK before transmitting the next frame. The sending device is equipped with a timer which indicates how long it should take for an acknowledgement to comeback. If none is received within the allotted time period, the source assumes the last data frame was lost in transit and retransmits it. Because the stop-and-wait mechanism is very inefficient, it is not widely used.

(ii) Go-back-N ARQ – Go-back-N ARQ is based on the sliding window flow control, which is also known as continuous ARQ. In this technique, a series of data frames is transmitted continuously without waiting for an acknowledgement. Number N specifies the number of successive frames which can be transmitted in the absence of an ACK or a NAK. If receiving station detects an error in a frame, it transmits a NAK to the transmitter for that frame. Then, receiver discards all further incoming frames, whether or not they are good, and now waits to receive correctly the frame which was in error before accepting any other frames.

When the transmitting station receives a NAK, it must retransmit the frame in question plus all succeeding frames. Therefore, the name go-back-N, because frames which were transmitted after the damaged frame also must be retransmitted. When an error takes place, this may affect up to N previously transmitted frames. As is the case with stop-and-wait ARQ, the go-back-N ARQ uses a timer mechanism which informs the transmitter how long it should wait for an acknowledgement to come back before it resends unacknowledged frames.

(iii) Selective-repeat ARQ – In selective-repeat ARQ, only the specific lost or damaged frame is resent. Intuitively this may appear more efficient than the go-back-N ARQ, where all good frames following the error are also resent. Although this does provide better performance, the implementation can be quite involved. The reason is that the receiver has

the additional major burdens of storing frames which follow an e keeping track of which frame was incorrect, and inserting. The co retransmitted frame into the appropriate sequence when it arrives. Be the additional logic required for such functions is costly and comple implement, selective-repeat ARQ is used much less as compared to back-N ARQ.

Q.27. Explain the noisy channel protocol – Go-back-N ARQ. ***(R.G.P.V., Dec.***

Ans. Refer the ans. of Q.26 (ii).

Q.28. Explain the mechanism of stop and wait ARQ. ***(R.G.P.V., June***

Ans. Stop-and-wait flow control technique is the base of stop-and- ARQ. A single frame is transmitted by the source station and then so station must await an acknowledgement (ACK). Until the destination station's reply arrives at the source station, no other data frames can be transmitted.

Two types of errors could occur. First, the frame which arrives at the destination could be damaged. By using the error-detection technique, the receiver detects this and simply discards the frame. Source station is equipped with a timer to account for this possibility. After the transmission of a frame, the source station waits for an acknowledgement. In the condition, when no acknowledgement is received by the time that timer expires, then the same frame is sent again. It should be noted that this method needs that the transmitter maintains a copy of a transmitted frame until an acknowledgement is received for that frame.

Damaged acknowledgement is the second type of error. This

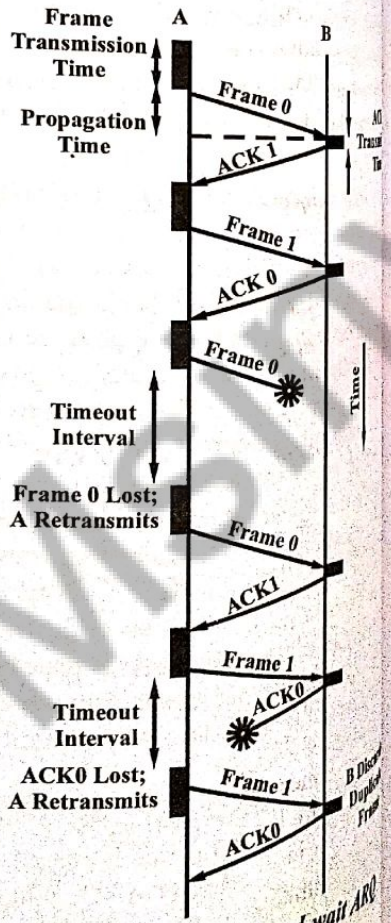


Fig. 2.17 Stop-and-wait ARQ

can be cleared from the following situation. Station A transmits a frame. Station B receives correctly the frame that responds with an acknowledgement (ACK). In transit, the ACK is damaged and is not identified by A, which will, therefore, time-out and retransmit the same frame. This duplicate frame arrives and is received by B. Therefore, B has received two copies of the same frame as if they were separate. For avoiding this problem, frames are alternately labeled with 0 and 1 and positive acknowledgements are of the form ACK0 and ACK 1. In keeping with the sliding-window convention, an ACK0 acknowledges receipt of a frame numbered 1 and shows that the receiver is ready for a frame number 0.

An example of the use of stop-and-wait ARQ is given in fig. 2.17 which shows the transmission of a sequence of frames from source A to destination B. Above described two types of errors are shown in the figure. The third frame transmitted by A is lost or damaged and thus no acknowledgement is returned by B. A times out and the frame is retransmitted. Later, a frame labelled 1 is transmitted by A but the ACK0 for that frame is lost. A times out and the same frame is retransmitted. If B receives two frames in a row with the same label, then it discards the second frame but transmits back an ACK0 to each.

The main benefit of stop-and-wait ARQ is its simplicity. Its main disadvantage is that stop-and-wait is an inefficient mechanism.

Q.29. Discuss and compare DLL "Go-back-N" and "Selective Repeat" protocols. ***(R.G.P.V., Dec. 2017)***

Or

With the aid of frame sequence diagrams and assuming a selective repeat error control scheme, describe how the following are overcome using both implicit and explicit retransmission –

(i) A corrupted information frame

(ii) A corrupted ANCK/NAK frame.

Ans. **Protocol Using Go-back-N** – If we have short frames, requiring a long transit (propagation) time and a high bandwidth line then it will result in low utilization of bandwidth because the sender waits for an acknowledgement before sending another frame. A much better efficiency can be achieved if the sender is allowed to transit upto w frames before blocking, instead of just 1. With an appropriate choice of w the sender will be able to continuously transmit frames for a time equal to the round-trip transit time without filling up the window. This technique is called the ***pipelining***.

When frames are pipelined over an unreliable communication channel, certain errors are bound to occur. There are two basic approaches adopted to deal with error in the presence of ***pipelining***.

The first strategy is called ***go-back-N,*** where the receiver simply discards all subsequent frames, sending no acknowledgements for the discarded frames.

This strategy corresponds to a receive window of size 1. In other words data link layer refuses to accept any frame except the next one it must give the network layer. The pipeline will begin to empty when the sender's window fills up before the timer runs out. Eventually, the sender will time out and retransmit all unacknowledged frames in order, starting with the damaged lost one. This approach can waste a lot of bandwidth when the error rate high. This is shown in fig. 2.18.

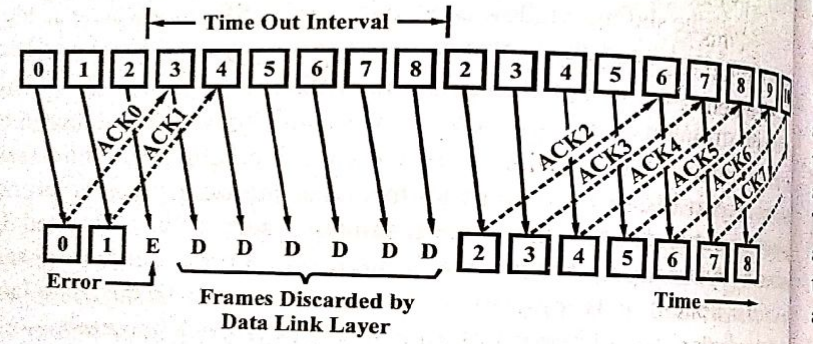


Fig. 2.18

The other general strategy for handling errors, when frames are pipelined is called ***selective repeat*** where the receiving data link layer store all the correct frames following the bad one. If the sender finally notices that something wrong, it just retransmits the one bad frame, not all its successors. When second try succeeds, the receiving data link layer will now have many correct frames in sequence, so they can all be handed off to the network layer quickly and the highest number acknowledged. This strategy corresponds to a receive window larger than 1. Any frame within the window may be accepted when buffered until all the preceding ones have been passed to the network layer. When the window is large, this approach can need large amounts of data link layer memory. The user can choose among the two according to his application requirements. This approach is depicted in fig. 2.19.

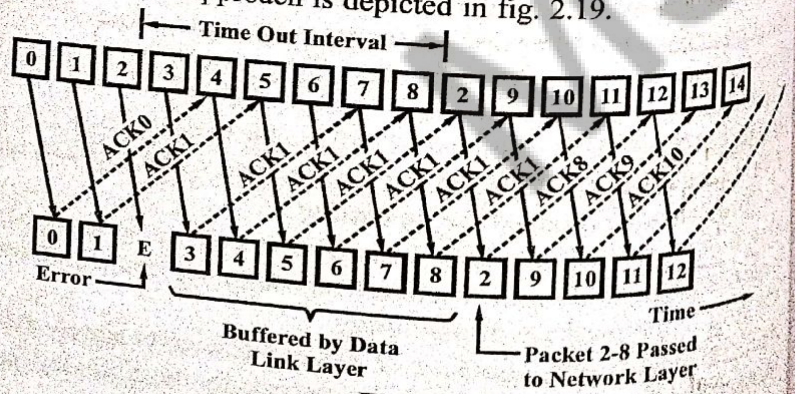


Fig. 2.19

In this protocol, we do not assume that the network layer has infinite supply of packets to send instead whenever it has a packet to send, it can cause a network-layer-ready event to happen. However, in order to enforce flow control rule the data link layer uses the enable-network-layer and disable-network-layer procedures to prevent network layer to overburden it with more packets. At any time, the number of unacknowledged frames should not be more than Max-Seq.

Although this protocol do not buffer the frames arriving after an error but the sender must keep track of all transmitted frames until it gets an acknowledgement by the receiver that they have been accepted as it may have to retransmit all unacknowledged frames later. All the previous frames are automatically acknowledged when an acknowledgement comes for frame n. This property is specially important when some of the previous acknowledgements were lost or garbled. When an acknowledgement arrives the data link layer checks which buffered can be released and proceeds by accepting more packets from network layer.

Since there are multiple outstanding frames, it logically needs multiple timers, one per outstanding frame. Each frame times out independently of all the other ones. All of these timers can easily be simulated by software, using a single hardware clock that causes interrupt periodically. The pending time outs form a linked list, with each node of list telling how many times the clock ticks before the timer goes off, the frame being timed, and pointer to the next node.

The implementation of timer can be understood with the help of fig. 2.20 (a). Let us consider the clock ticks once every 100 msec. Initially, the real time is 10 : 00 : 00.0 and there are three timeouts are pending, at 10 : 00 : 00.5, 10 : 00 : 01.3 and 10 : 00 : 01.9. Every time the hardware clock ticks, the real time is updated and the tick counter at the head of the list is decremented. When the tick counter becomes zero, a timeout is caused and the node removed from the list, as shown in fig. 2.20 (b).

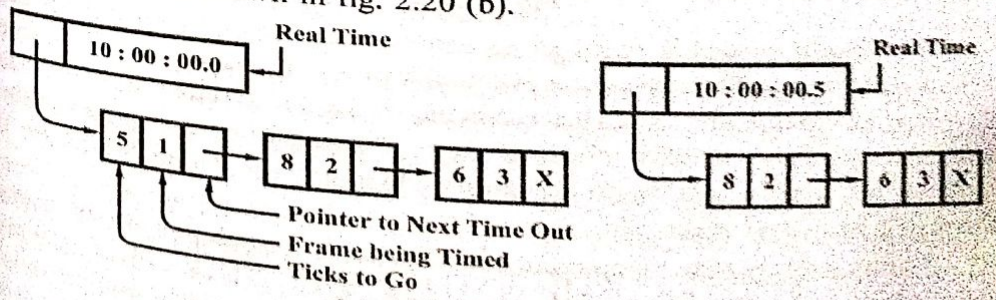


Fig. 2.20 Simulation of Multiple Timers in Software

A Protocol Using Selective Repeat – The above protocol works well when errors are rare, but when the line is poor it wastes a lot of bandwidth on

retransmitted frames. An alternative strategy for handling errors is to allow the receiver to accept and buffer the frames following a damaged or lost one until that frame is correctly received and then all the frames are handed to the network layer in correct sequence. Such a protocol does not discard nearly because an earlier frame was damaged or lost.

In this protocol, both transmitter and receiver maintain a window of acceptable sequence numbers. The transmitter's window size starts at 0 and grows to MAX_SEQ. The receiver's window is always fixed in size equal to MAX_SEQ. The receiver has a buffer reserved for each sequence number within its fixed window. There is a bit associated with each buffer which tells whether the buffer is full or empty. Whenever a frame arrives its sequence number is examined to check whether it lies within the window. If so, and if it is not received earlier, it is accepted and stored. It is passed to the network layer only when all the lower numbered frames have been delivered to the network layer in correct order.

Non-sequential receive introduces certain problems. For example, suppose have 3 bit sequence number, then the transmitter is allowed to transmit seven frames before, being required to wait for an acknowledgement. The initial position of transmitter and receiver window is illustrated in fig. 2.21 ahead. The transmitter transmits frames 0 through 6. All seven frames correctly, so the receiver acknowledges them and advances its window allow receipt of 7, 0, 1, 2, 3, 4, or 5 as illustrated in fig. 2.21 (b). All buffers are marked empty.

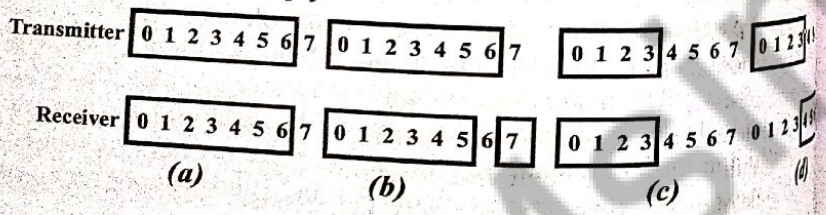


Fig. 2.21

Now suppose at this point same error creeps in, wiping out all acknowledgements. The transmitter eventually times out and retransmits frame 0. When this frame arrives at the receiver, it checks whether the frame within the receiver's window. Unfortunately, it is so will be accepted and receiver will send a piggybacked acknowledgement for frame 6 because through 6 have been received.

The transmitter now being conformed of correct transmission advances its window and sends frames 7, 0, 1, 2, 3, 4 and 5. The receiver accepts frame 7 and its packet will be passed directly to the network layer. Immediately after this the receiving data link layer checks if it has a valid frame 0. In case, it has and passes the packet within to the network layer. Consequently the network layer gets an incorrect packet and the protocol fails.

The problem is that after the receiver advanced its window, the new range of valid sequence numbers overlapped the old one. The receiver is unable to distinguish between original frames and the duplicate ones, the solution to this problem is to avoid the window overlapping after the receiver advances its window. The maximum window size should be at most half the range of the sequence numbers to ensure that there is no overlap, as shown in fig. 2.21 (c) and (d). For example, if three bits are used for sequence number than maximum window size will be 4. In general, the window size for protocol 6 will be (MAX_SEQ + 1)/2.

For a K-bit sequence number field, with sequence number range of 2^K, the maximum size of window for selective repeat is 2^{K-1}.

In selective repeat, the maximum window size should be no more than half the range of sequence numbers.

The receiver will never accept frames whose sequence numbers are above the upper edge of the window. Consequently, the number of buffers needed is equal to the window size, not the range of sequence numbers. For the same reason, the number of timers needed is equal to the number of buffers, not to the size of the sequence space.

In the previous protocol, we have assumed that the channel is heavily loaded. The acknowledgement were not send immediately instead then were piggybacked onto the next data frame. If the reverse traffic is light, the acknowledgements will be delayed. If the forward traffic is high and backward traffic is negligible, only MAX_SEQ packets are sent and then the protocol blocks.

In this protocol, this problem is eliminated. After an in-sequence data frame arrives, an auxiliary timer is started by start_ack_timer. If no reverse traffic is encountered before this timer goes off, a separate acknowledgement frame is sent. With this arrangement, one-directional traffic flow is possible, because the lack of reverse data frames onto which acknowledgements can be piggybacked is no longer an obstacle.

The timeout associated with the auxiliary timer should be appreciably shorter than the timer used for timing out data frames so that the acknowledgement for a correctly received frame arrives before the transmitter times and retransmits the frame.

This protocol is more robust in the case of errors. Whenever the receiver suspects some errors it sends a negative acknowledgement (NAK) frame back to the transmitter. Such a frame is a request for retransmission of the frame specified in the NAK. To avoid making multiple requests for retransmission of the same last frame, the receiver should keep track of whether a NAK has already protocol 6 is true if no NAK has been sent yet for frame-expected. If the NAK gets mangled or lost, no harm is done, because the transmitter will eventually time out and retransmit the missing frame anyway.

In some cases, the time needed for (frame propagation + process... acknowledgement coming back) is constant. In such cases, the trans... can adjust its timer a slightly larger than the sum of above 3 times. If this ... is highly variable, then the transmitter can either set the timer value sma... risk unnecessary retransmissions or set it to a large value and waste band... In general whenever the standard deviation of the acknowledgement int... is small compared to the interval itself, the timer can be set "tight" and N... are not useful otherwise the timer must be set "loose" and NAKs can appre... speed up retransmission of lost or damaged frames.

Q.30. Describe the working of a selective repeat protocol. ***(R.G.P.V., June ...***

Or

Explain Go-back-N protocol in detail. ***(R.G.P.V., Dec. ...***

Ans. Refer the ans. of Q.29.

Q.31. Discuss the various performance issues of ARQ techniques.

Ans. First, we take ***stop-and-wait ARQ***. When there is no error, maximum utilization is 1/ (1 + 2a). It is desired to account for the poss... that some frames are repeated due to bit errors. Utilization can be given ...

$$u = \frac{T_f}{T_t}$$

where, T_f = Time for transmitter to emit a single frame

T_t = Total time that line is engaged in the transmission of a single f...

For error-free operation using stop-and-wait ARQ,

$$u = \frac{T_f}{T_f + 2T_p}$$

where, T_p = Propagation time.

If errors happen, equation (i) must be modified to –

$$u = \frac{T_f}{N_r\ T_t}$$

where, N_r = Expected number of transmissions of a frame.

Therefore, for stop-and-wait ARQ –

$$u = \frac{1}{N_r(1+2a)}$$

By considering the probability P that a single frame is in error, a ... expression of N_r can be obtained. When it is assumed that ACKs and ... are never in error, the probability that it will take exactly k attempts to ... frame successful is $P^{k-1}(1 - P)$. That is, (k – 1) unsuccessful attempts ...

followed by one successful attempt. The probability of this happening is just the product of the probability of the individual events happening. Then –

$$N_r = E[\text{transmissions}]$$

$$= \sum_{i=1}^{\infty} \left(i \times P_r[i \text{ transmissions}]\right) = \sum_{i=1}^{\infty} \left(i P^{i-1}(1-P)\right) = \frac{1}{1-P}$$

Therefore, for ***stop-and-wait*** –

$$\mathbf{u = \frac{1-P}{1+2a}}$$

In the case of selective-repeat ARQ, the same reasoning is used as applied to stop-and-wait ARQ, which is, the error-free equations must be divided by N_r. Here, $N_r = \frac{1}{1-P}$. Therefore, ***for selective-repeat*** –

$$\mathbf{u} = \begin{cases} \mathbf{1-P}, & \mathbf{W \geq 2a+1} \\ \mathbf{\dfrac{W(1-P)}{2a+1}}, & \mathbf{W < 2a+1} \end{cases}$$

The same reasoning is applied to go-back- N ARQ, but N_r is approximating more carefully. Every error produces a need to retransmit k frames rather than just one frame.

Therefore, N_r = E [number of transmitted frames to successfully transmit one frame]

$$= \sum_{i=1}^{\infty} f(i) P^{i-1}(1-P)$$

where, f (i) = Total number of frames transmitted if the original frame must be sent i times. This can be written as

$$f(i) = 1 + (i-1)K = (1-K) + Ki$$

Substituting yields,

$$N_r = (1-K)\sum_{i=1}^{\infty} P^{i-1}(1-P) + K\sum_{i=1}^{\infty} iP^{i-1}(1-P)$$

$$= 1 - K + \frac{K}{1-P} = \frac{1-P+KP}{1-P}$$

Here, $K \approx (2a+1)$ for $W \geq (2a+1)$ and $K = W$ for $W < (2a+1)$. Therefore, for go-back-N –

$$\mathbf{u} = \begin{cases} \mathbf{\dfrac{1-P}{1+2aP}}, & \mathbf{W \geq 2a+1} \\ \mathbf{\dfrac{W(1-P)}{(2a+1)(1-P+WP)}}, & \mathbf{W < 2a+1} \end{cases}$$

MSInventer

It should be remembered that for W =1, both selective-repeat and go-back-N ARQ become stop-and-wait. Comparison for these three control techniques for a value of $P = 10^{-3}$ is shown in fig. 2.22.

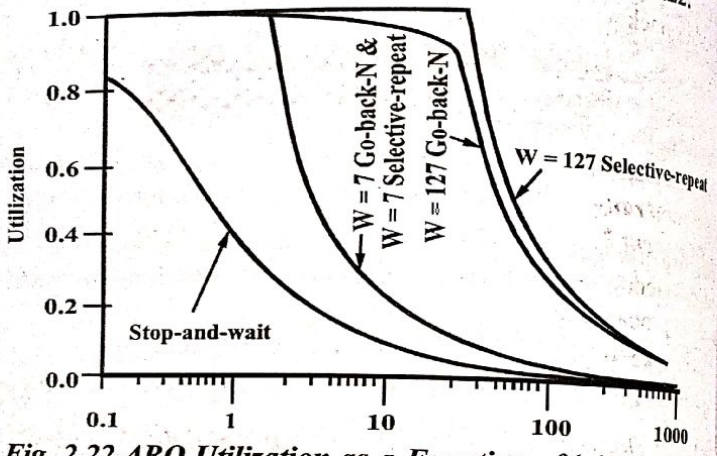


Fig. 2.22 ARQ Utilization as a Function of 'a' ($P = 10^{-3}$)

Q.32. Compare the performance of stop-and-wait protocol and sliding window protocol. ***(R.G.P.V., Dec. 2014,***

Ans. Refer the ans. of Q.25 and Q.31.

Q.33. Explain hybrid ARQ (HARQ) technique in detail.

Ans. Hybrid ARQ (HARQ) is performed by both the media access control (MAC) layer and the physical layer. This crosslayer processing has become popular in recent years and represents a gradual shift toward more cooperation between protocol layers to enhance performance. In traditional ARQ, if the MAC layer detects an error in a packet, it would discard the erroneous packet and request retransmission. However, potentially useful information could in the erroneous packet is thrown away. In HARQ, if the MAC layer detects an error in a packet, it would still send a NAK to request retransmission when the newly retransmitted packet arrives, the physical layer would combine this retransmitted packet with the original packet to yield more information forward error control (FEC) decoding. If the combined packet passes then the receiver sends an ACK and HARQ process ends. If the combined packet still does not pass the CRC, then the receiver sends a NAK to request another retransmitted packet to be used by HARQ. The combining of packets takes place prior to FEC decoding, and FEC decoding operates on the combined packet.

HARQ are of two types, namely, chase combining and incremental redundancy. In chase combining, the bits in the subsequently retransmitted packets are FEC coded the same way as those in the original packet. However, in incremental redundancy, the bits in the subsequently retransmitted packet are FEC coded differently from those in the first packet. The idea is that the redundancy bits previously punctured out are incrementally sent with each retransmitted packet.

NUMERICAL PROBLEMS

Prob.1. A channel has bit rate of 4 kbps and a propagation delay of 20 m sec. For what range of frame sizes does stop and wait give an efficiency of at least 50 percent ? ***(R.G.P.V., Dec. 2003, 2004, June 2012, Dec. 2012)***

Sol. Efficiency will become 50% when the time to transmit the frame = Round trip propagation delay.

160 bits take 40 ms at a transmission rate of 4 bits/ms.

For frame sizes ***above 160 bits,*** stop-and-wait is reasonably efficient. **Ans.**

Prob.2. A channel of one Mbps with propagation delay of 270 ms transmits frames of size 1000 bits. What is the maximum link utilization for stop-and-wait, and sliding window with window size 7 ? ***(R.G.P.V., June 2015)***

Sol. Given that

Bit rate = 1 Mbps = 10^6 bps

Propagation delay (t_p) = 270 ms = 270×10^{-3} sec = 0.270 sec

Frame size = 1000 bits

and Window size (W) = 7

We know that,

$$t_f = \frac{\text{Frame size}}{\text{Bit rate}} = \frac{1000}{10^6} = 10^{-3} = 0.001 \text{ sec}$$

Number of packet accommodated in a channel (a) is given by

$$a = \frac{\text{Propagation time } (t_p)}{\text{Frame transmission time } (t_f)}$$

$$= \frac{0.270}{0.001} = 270$$

The maximum link utilization for stop-and-wait is given by

$$u = \frac{1}{1+2a} = \frac{1}{1+2\times 270} = \frac{1}{1+540}$$

$$= 1.848 \times 10^{-3} = \mathbf{0.185\%}$$ **Ans.**

The maximum link utilization for sliding window is given by

$$u = \frac{W}{2a+1} = \frac{7}{2\times 270+1}$$

$$= 0.01294 = \mathbf{1.294\%}$$ **Ans.**

Prob.3. Given an error free 64 kbps satellite channel which is used to send 512 bytes data frames in one direction with very short acknowledgements coming back the other way. What will be the maximum throughput for window size of 1, 7, 15 and 127 ? ***(R.G.P.V., June 2011,***

Sol. Time for 512 byte frame (4096 bits) to fill the channel

$$= \frac{4096}{64000} \text{ sec}$$

$$= 0.064 \text{ sec}$$

$$= 64 \text{ m sec}$$

Propagation time, $t_p = 250$ m sec

Thus to keep the channel busy window needs is of $\frac{250}{64} = 3.91 \simeq 4$ fra

With a window size of (1 frame) 4096 bits per 250 msec can be sent a throughput of = **164 bps**

For a window above 4 frames, the maximum throughput is 64 kbps

Prob.4. What is remainder obtained by dividing $x^7 + x^5 + 1$ by generator polynomial $x^3 + 1$? ***(R.G.P.V., June***

Sol. Data to be divided –

Polynomial = $x^7 + x^5 + 1$

In binary = 10100001

Divisior –

Polynomial = $x^3 + 1$

In binary = 1001

```
1001)10100001(10110
     1001
     ----
      0110
      0000
      ----
       1100
       1001
       ----
        1010
        1001
        ----
         0111
         0000
         ----
          111
```

The remainder obtained by dividing $x^7 + x^5 + 1$ by the generator polynomial $x^3 + 1$ is **111**.

PROTOCOL VERIFICATION – FINITE STATE MACHINE MODELS & PETRI NET MODELS

Q.34. What do mean by protocol verification ? ***(R.G.P.V., June 2015)***

Ans. During the all phases of design, validation activity is necessary and may contain testing of the final system implementation, analytical performance predictions, and verification. Verification is dependent on the system specification, and involves logical reasoning. Hence, it is employed during the design phase before any system implementation exist, to eliminate possible design problems.

The somewhat ambiguous term protocol verification is generally used to mean this first design verification problem. Protocol verification design takes on a characteristics communication oriented flavor, since protocols are inherently systems of concurrent independent entities interacting through exchange of messages. Although, protocol verification is generally performed by various models i.e., finite state machine models and petri net models.

Q.35. Explain the finite state machine model for protocol verification. ***(R.G.P.V., June 2013)***

Ans. The finite state machine is a mainly used in several protocol models. With this technique, every ***protocol machine*** (i.e., transmitter or receiver) is always in a particular state at every time instant. Its state consists of all the values of its variables, including the program counter.

The combination of all the states of the two protocol machines and the channel is known as state of the complete system. The channel state is obtained by its contents. Using protocol 3 as an example, the channel has four possible states – a 0 frame or a 1 frame moving from transmitter to receiver, an acknowledgement frame going the other way, or an empty channel. The complete system has 16 distinct states when we model the transmitter and receiver as each consisting two states.

From every state, there are zero or more possible ***transitions*** to other states. When some event happens, transitions take place. In case of a protocol machine, a transition might take place if a frame is transmitted, if a frame arrives, if a timer expires, if an interrupt takes place, etc. For the channel, typical events are insertion of a new frame onto the channel by a protocol machine, delivery of a frame to a protocol machine, or loss of a frame because of noise burst. Given a complete description of the protocol machines and the channel characteristics, it is possible to sketch a directed graph representing all the states as nodes and all the transitions as directed arcs.

One particular state is designated as the ***initial state.*** This state corresponds to the description of the system when it starts running, or at some convenient

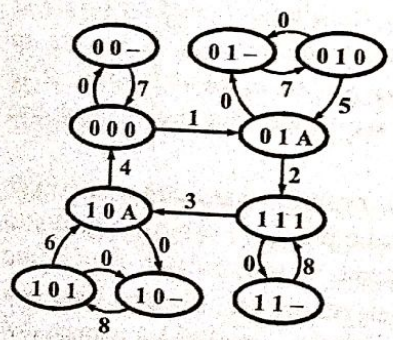
visionet

starting place shortly thereafter. From the initial state, some, perhaps
the other states may be approached by a sequence of transitions. Using
known techniques from graph theory (e.g., computing the transitive
of a graph), it is possible to determine which states are reachable and
are not. This technique is called ***reachability analysis***. This analysis
helpful in determining whether a protocol is correct.

All processes are in their initial states at the starting of time. Then
start to happen, like frames becoming available for transmission or timers
off. To take an action and switch to a new state each event can cause one
processes or the channel. One can construct the reachability graph and
the protocol, by carefully enumerating every possible successor to each

In the protocol specification, reachability analysis is used to detect
of errors. For example, when this is possible for a specific frame to take
in a specific state and the FSM does not say what action must be
specification is in error (incompleteness). If there exists a set of states
which no exit can be made and from which no progress can be made (i.e.
correct frames can be received any more), we have another error (deadlock).
The protocol specification is a less serious error that tells how to
event in a state where the event cannot take place (extraneous
Other errors are also detected.

Consider a finite state machine model is shown in fig. 2.23 (a).
graph corresponds to protocol 3 as described above – every protocol
has two states and the channel has four states. A total of 16 states exist,
of them reachable from the initial one. In this figure, the unreachable
not represented. For simplicity, checksum errors can also be avoided



(a) State Diagram for Protocol 3

Transition	Who runs ?	Frame accepted	Frame emitted
0	–	(Frame lost)	
1	R	0	A
2	S	A	1
3	R	1	A
4	S	A	0
5	R	0	A
6	R	1	A
7	S	(timeout)	0
8	S	(timeout)	1

(b) Transitions

Fig. 2.23

The three characters, SRC label each state, where S is 0 or 1, equiv
to the frame the transmitter is trying to transmit; R is also 0 or 1, equiv
the frame the receiver expects, and C is 0,1, A, or empty (–), equivalent

state of the channel. In this case, the initial state has been selected as (000). This means that the transmitter has just transmit frame 0, the receiver expects frame 0, and frame 0 is currently on the channel.

Fig. 2.23 shows a nine type of transitions. Transition 0 made up of the channel losing its contents and transition 1 made up of the channel correctly delivering packet 0 to the receiver, with the receiver then varying its state to expect frame 1 and emitting an acknowledgement. For network layer transition 1 also corresponds to the receiver delivering packet 0 to the network layer. Fig. 2.23 (b) lists the other transitions. Since it does not change the state (in protocol 3), the frame arrival with a check sum error has not been shown.

Transitions 1, 2, 3, and 4 are repeated in order over and over during normal operation. In case of each cycle, two packets are delivered, bringing the transmitter back to the initial state of trying to transmit a new frame with sequence number 0. It makes a transition from state (000) to state (00 –) if the channel loses frame 0. Eventually, the transmitter times out (transition 7) and the system moves back to (000). The loss of an acknowledgement is more complicated, requiring two transitions, 7 and 5, or 8 and 6, to repair the damage.

One of the properties that a protocol with a 1-bit sequence number must have is that no matter what sequence of events happens, the receiver never delivers two odd packets without an intervening even packet, and vice versa. From the graph of fig. 2.23, we see that this requirement can be stated more formally as "there must not exist any paths from the initial state on which two occurrences of transition 1 occur without an occurrence of transition 3 between them, or vice versa". From the figure, it can be seen that the protocol is correct in this respect.

A similar requirement is that there is not exist any paths on which the sender changes state twice (e.g., from 0 to 1 and back to 0) while the receiver state remains constant. Were such a path to exist, then in the corresponding sequence of events, two frames would be irretrievably lost without the receiver noticing. The packet sequence delivered would have an undetected gap of two packets in it.

The another important property of a protocol is the absence of deadlocks. A ***deadlock*** is a situation where the protocol can make no more forward progress (i.e., deliver packets to the network layer) no matter what sequence of events happens. In terms of the graph model, a deadlock is characterized by the existence of a subset of states which is reachable from the initial state and that has two properties –

(i) There is no transition out of the subset

(ii) In the subset, there are no transitions that cause forward progress.

Once in the deadlock situation, the protocol remains there forever. Further, it is simple to see from the graph that protocol 3 does not suffer from deadlocks.

Q.36. Discuss Petri net model in detail. (R.G.P.V., June

Ans. A Petri net contain four basic elements – places, transitions and tokens. A ***place*** indicates a state which (part of) the system may be Petri net with two places, A and B, is shown in fig. 2.24, both show circles. The system is currently in state A, indicated by the ***token*** (heavy in place A. A ***transition*** is represented by a horizontal or vertical bar transition has zero or more ***input arcs*** coming from its input places, and or more ***output arcs,*** going to its output places.

When there is at least one input token in each of its input places, a tran is enabled. Any enabled transition may ***fire*** at will, removing one token every input place and depositing a token in every output place. Tokens w be conserved when the number of input arcs and output arcs differs. two or more transitions are enabled, any one of them may fire. The sele of a transition to fire is indeterminate, that is why Petri nets are useful modeling protocols. The Petri net of fig. 2.24 is deterministic and is employed to model any two-phase process (e.g., the behaviour of a baby – eat, sleep, eat, sleep, and so on). As with all modeling tools, unnecessary detail is suppressed.

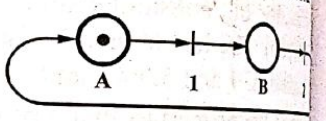


Fig. 2.24 A Petri Net with T Places and Two Transition

The Petri net model using protocol 3 is given in fig. 2.25. Unlike finite state machine model, there are no composite states here; the sender state, channel state, and receiver's state are represented separately. In 2.25, horizontal and vertical line shows the transitions. Transitions 1 correspond to transmission of frame 0 by the sender, normally, and timeout respectively. Transitions 3 and 4 are analogous for fram Transitions 5, 6 and 7 correspond to the loss of frame 0, an acknowledgm and frame 1, respectively. When a data frame with the wrong seque number arrives at the receiver, transitions 8 and 9 occur. Transitions 1 11 show the arrival at the receiver of the next frame in sequence an delivery to the network layer.

Petri nets may be employed to detect protocol failures in a way simil the use of finite state machines. For example, the protocol would be in when some firing sequence included transition 10 twice without transitio intervening. In a Petri net, the concept of a deadlock is similar to finite machine.

Petri nets may be indicated in convenient algebraic form resembl grammar. Each transition contributes one rule to the grammar. The input output places of the transition is specified by each rule. Since fig. 2.25 transitions, its grammar has 11 rules, numbered 1-11, each one corresp to the transition with the same number. The grammar for the Petri net

2.25 is as follows –

1 : BD → AC 2 : A → A 3 : AD → BE 4 : B → B
5 : C → 6 : D → 7 : E → 8 : CF → DF
9 : EG → DG 10 : CG → DF 11 : EF → DG

It is interesting to note how we have managed to reduce a complex protocol to 11 simple grammar rules that can easily be manipulated by a computer program.

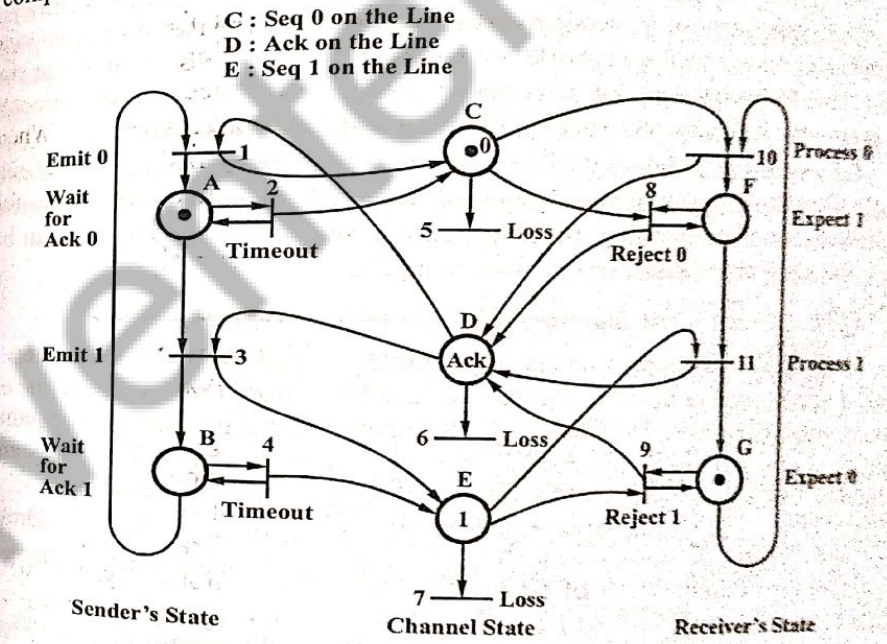


Fig. 2.25 A Petri Net Model for Protocol 3

The current state of the Petri net is represented as an unordered collection of places, each place represented in the collection as many times as it has tokens. Any rule, all of whose left-hand side places are present can be fired, removing those places from the current state, adding its output places to the current state. The marking of fig. 2.25 is ACG, (i.e., A, C and G each have one token). Consequently, rules 2, 5 and 10 are all enabled and any of them can be applied, leading to a new state (possibly with the same marking as the original one). In contrast, rule 3 (AD → BE) cannot be applied because D is not marked.

ARP/RARP/GARP

Q.37. Discuss address mapping in brief.

Ans. A packet starting from a source host may pass through several different

physical networks before finally reaching the destination host. The l
routers are recognized at the network level by their logical (IP) addre

However, packets pass through physical networks to reach the
and routers. At the physical level, the hosts and routers are recognized
physical addresses. A physical address is a local address. It must b
locally, but is not necessarily unique universally. It is called a physica
because it is usually (but not always) implemented in hardware.

The physical address and the logical address are two different ide
We need both because a physical network such as Ethernet can h
different protocols at the network layer such as IP and IPX (Novell
same time. Likewise, a packet at a network layer such as IP may pass t
different physical networks such as Ethernet and localTalk (Apple).

This means that delivery of a packet to a host or a router requi
levels of addressing – logical and physical. We need to be able to map
address to its corresponding physical address and vice versa. These
done by using either static or dynamic mapping.

Q.38. Discuss static mapping and dynamic mapping in brief.

Ans. Static mapping involves in the creation of a table that asso
logical address with a physical address. This table is stored in each mac
the network. Each machine that knows, for example, the IP address of a
machine but not its physical address can look it up in the table. This ha
limitations because physical addresses may change in the following way

(i) A machine could change its NIC, resulting in a new physical a

(ii) In some LANs, such as LocalTalk, the physical address ch
every time the computer in turned on.

(iii) A mobile computer can move from one physical netw
another, resulting in a change in its physical address.

To implement these changes, a static mapping table must be u
periodically. This overhead could affect network performance.

In ***dynamic mapping*** each time a machine knows one of th
addresses i.e., logical or physical, it can use a protocol to find other o

A mapping between physical and logical addresses is done using pro
IP packets use logical addresses. However, these packets require
encapsulated in a frame, which requires physical addresses. A protocol
ARP (address resolution protocol), is designed for this purpose. We some
need reverse mapping – mapping a physical address to a logical addres
example when booting a diskless network or leasing an IP address to
Three protocols are designed for this purpose – RARP, BOOTP and D

Lack of flow and error control in the Internet Protocol has re
another protocol ICMP, that provides alerts. It reports congestion an
types of errors in the network or destination host.

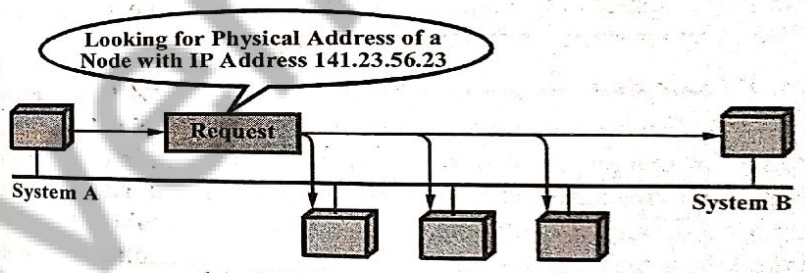
IP was originally designed for unicast delivery. As the Internet has evolved, a protocol called IGMP gives IP a multicast delivery capability.

Q.39. Explain the logical to physical address mapping in brief.

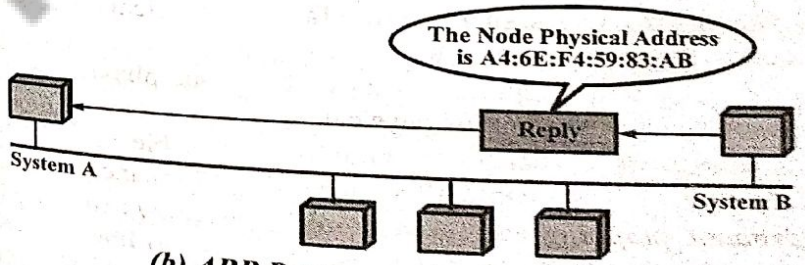
Or

Write a short note on ARP.

Ans. Anytime a host or router has an IP datagram to send to another host or router, it has the logial (IP) address of the receiver. The logical (IP) address is obtained from the DNS, if the sender is the host or it is found in a routing table if the sender is a router. But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver. The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network (see fig. 2.26).



(a) ARP Request is Broadcast



(b) ARP Reply is Unicast

Fig. 2.26 ARP Operation

Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packet.

In fig. 2.26 (a), the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not

know the physical address of the recipient. It uses the services of asking the ARP protocol to send a broadcast ARP request packet the physical address of a system with an IP address of 141.23.56.2

This packet is received by every system on the physical net only system B will answer it, as shown in fig. 2.26 (b). System B ARP reply packet that includes its physical address. Now system A all the packets it has for this destination by using the physical address

Q.40. Explain the packet format of an ARP.

Ans. The format of an ARP packet is shown in fig. 2.27.

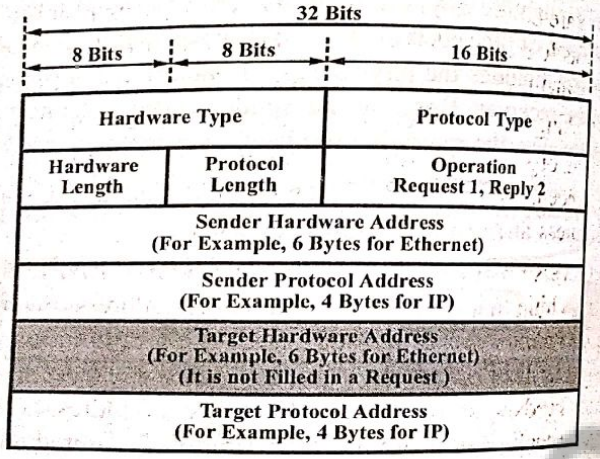

32 Bits
8 Bits
8 Bits
16 Bits
Hardware Type
Protocol Type
Hardware Length
Protocol Length
Operation Request 1, Reply 2
Sender Hardware Address (For Example, 6 Bytes for Ethernet)
Sender Protocol Address (For Example, 4 Bytes for IP)
Target Hardware Address (For Example, 6 Bytes for Ethernet) (It is not Filled in a Request)
Target Protocol Address (For Example, 4 Bytes for IP)

Fig. 2.27 ARP Packet

The fields are as follows –

(i) Hardware Type – This is a 16-bit field defining the ty network on which ARP is running. Each LAN has been assigned a based on its type. For example, Ethernet is given type 1. ARP can b any physical network.

(ii) Protocol Type – This is a 16-bit field defining the proto example, the value of this field for the IPv4 protocol is 0800_{16}. AR used with any higher-level protocol.

(iii) Hardware Length – This is an 8-bit field defining the the physical address in bytes. For example, for Ethernet the value is

(iv) Protocol Length – This is an 8-bit field defining the the logical address in bytes. For example, for the IPv4 protocol the v

(v) Operation – This is a 16-bit field defining the type of Two packet types are defined ARP request 1 and ARP reply 2.

(vi) Sender Hardware Address – This is a variable-leng defining the physical address of the sender. For example, for Ethe field is 6 bytes long.

(vii) Sender Protocol Address – This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.

(viii) Target Hardware Address – This is a variable-length field defining the physical address of the target.

(ix) Target Protocol Address – This is a variable-length field defining the logical address of the target. For the IPv4 protocol, this field is 4 bytes long.

Q.41. Explain the physical to logical address mapping. Also discuss the RARP protocol.

Ans. There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases –

(i) A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.

(ii) An organization does not have enough IP addresses to assign to each station, it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.

RARP (Reverse Address Resolution Protocol) – RARP finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.

However, a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.

A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply. The requesting machine must be running a RARP client program, the responding machine must be running a RARP server program.

There is a serious problem with RARP – Broadcasting is done at the data link layer. The physical broadcast address, all 1s in the case of Ethernet, does not pass the boundaries of a network. This means that if an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet. This is the reason that RARP is almost obsolete. Two protocols BOOTP and DHCP are replacing RARP.

Q.42. Explain the brief encapsulation of ARP packet.

Ans. A data link frame is directly sum up by an ARP packet. An ARP packet is encapsulated in an Ethernet frame as shown in fig. 2.28. The type field indicates that the data carried by the frame are an ARP packet.

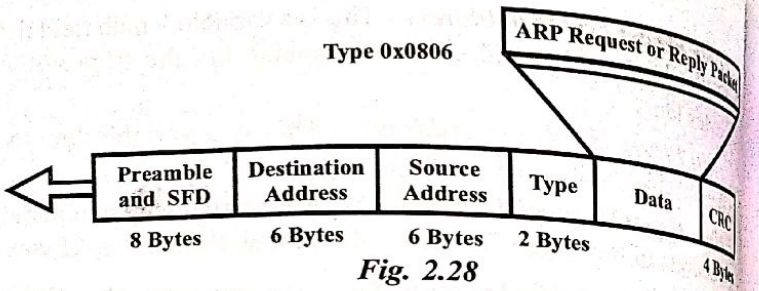


Fig. 2.28

Q.43. Write short note on GARP.

Ans. Gratuitous Address Resolution Protocol (GARP) requests pr duplicate IP address detection. A GARP request is a broadcast request router's own IP address. If a router sends an Address Resolution Pro (ARP) request for its own IP address and no ARP replies are receive router's assigned IP address is not being used by other nodes. If a r sends an ARP request for its own IP address and an ARP reply is receive router's assigned IP address is already being used by another node.

A GARP is an ARP broadcast in which the source and destination addresses are the same. It is used primarily by a host to inform the net about its IP address. A spoofed gratuitous ARP message can cause no mapping information to be stored incorrectly, causing a network malfu

GARP is a method of establishing an association between a logical IP a and a hardware address whenever an interface is created or the state interface shifts to the operationally up state. On the other hand, ARP dynam binds the IP address (the logical address) to the correct MAC addres device that transmits a GARP populates both the source and destination with its own information. The devices that receive the GARP request update the ARP caches with the new information contained in the GARP p

By default, updating the ARP cache on GARP replies is disabled router. On Ethernet interfaces, you can enable transmission of GARP on a specific interface by using the ip gratuitous-arps command in Configuration mode and specify the number of GARP packets to depending on the changes to IP interface settings. If an IP address is con directly on the physical Ethernet interface and a VLAN major interface configured on the Ethernet interface for VLAN encapsulation, transmis GARP packets does not take place.

UNIT 3

MAC SUBLAYER

MAC SUBLAYER – MAC ADDRESSING, BINARY EXPONENTIAL BACK-OFF (BEB) ALGORITHM

Q.1. What do you mean by medium access control sublayer ? Why do we need it ? Explain MAC. ***(R.G.P.V., June 2017)***

Ans. The protocol used to determine who goes next on a multiaccess channel belong to a sublayer of data link layer called the MAC sublayer. The medium access control (MAC) sublayer resolves contention on a shared-media LAN, which basically determines what devices can access the LAN media and when. The MAC sublayer includes synchronization, flow and error control procedures necessary for transporting information from one device to another, and physical address of the device to receive or route a frame. The MAC sublayer is where the LLC is encapsulated and passed on to the physical layer, where it is encoded and delivered to the transmission medium. At the destination, the MAC sublayer is removed from the transmission line, decoded, and passed on to the logic link control (LLC) for decapsulation. The MAC sublayer is also responsible for invoking CSMA/CD procedures. 803.2 MAC frames incorporate CRC-32 for error detection, which detects virtually all transmission errors. However, the MAC sublayer does not provide mechanisms for sequencing, acknowledging, or rejecting frames, making it an unreliable data link layer transport medium.

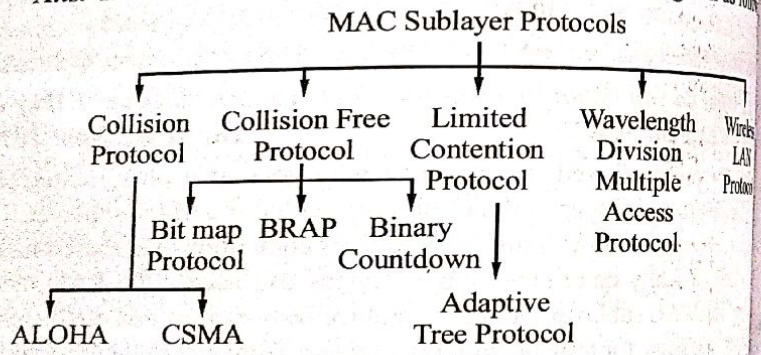
Main parameters in any medium access control technique are where and how. Where refers to whether control is exercised in a distributed or centralized manner. In a decentralized network, the stations collectively do a medium access control function to determine dynamically the order in which stations transmit. In a centralized network, a controller is designated which has the authority to grant access to the network. A station desiring to transmit must wait until it receives permission from the controller.

How is the second parameter which is constrained by the topology and is a trade-off among competing factors including performance, cost and complexity.

Generally, access control techniques can be categorized as being synch... or asynchronous. In synchronous techniques, a specific capacity is ded... to a connection. This is the same procedure used in circuit switching, freq... division multiplexing (FDM) and synchronous time-division multiplexing (T... Generally, these techniques are not optimal in LANs and MANs becau... requirements of the stations are unpredictable. It is preferable to have the ... to allocate capacity in an asynchronous (dynamic) manner, more or l... response to immediate demand. The asynchronous approach can be f... subcategorized as – round robin, reservation and contention.

Q.2. Write classification of MAC sublayer protocol. (R.G.P.V., June...

Ans. The classification of MAC sublayer protocol is given as follo...



Q.3. What is random access ? ***(R.G.P.V., Dec. ...***

Ans. Random access is the ability to access any item of data fr... population of addressable elements roughly as easily and efficiently a... other, no matter how many elements may be in the set. It is typically contr... to a sequential access. No station is superior to another and none is assi... the control over another in random access or contention methods. No st... allows, or does not allow, another station to transmit. At each instan... station which has data to transmit uses a procedure expressed by the pro... to make a decision on whether or not to transmit. This decision depen... the state of the medium (idle or busy).

Two features give random access method –

(i) There is no scheduled time for a station to send. Transm... is random between the stations. That is why these methods are know... random access.

(ii) No rules specify which station would transmit next. Sta... compete with one another to access the medium. That is why these pro... are also known as contention methods.

This method is evolved from a very interesting protocol called Al... which used a very simple procedure known as multiple access or random...

Q.4. Explain MAC addressing in detail.

Ans. The six-byte hardware address on the network interface card (NIC) is the MAC source address for the device. Source MAC addresses are always unicast addresses because more than one device cannot originate a transmission. On the other hand, the destination MAC address can be unicast, multicast or broadcast. A unicast destination address designates only one device as a recipient. The format for an IEEE 802.3 MAC address field is shown in fig. 3.1. The lower order bit (b_0) is always 0 in a unicast address. Thus, the hex value for the first byte is always an even number in a unicast address. In a MAC destination address field, the destination address is a unicast address, if the lower order bit is 0 and it is a multicast address, if the lower order bit is 1. Therefore, the first byte of a multicast address is always an odd number. The destination address is a broadcast address, if all 48 bits in the destination address field are 1s.

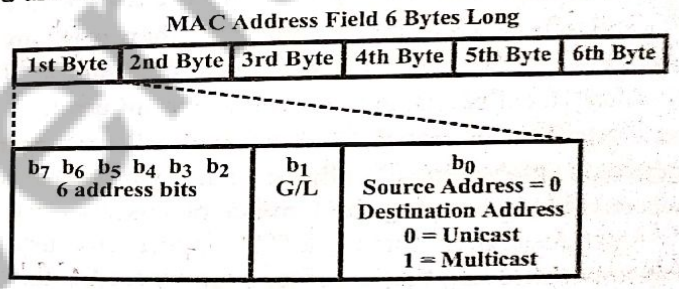


Fig. 3.1

MAC source hardware addresses can be globally unique or locally unique. Globally unique means that the address is unique for all LANs in existence. While, locally unique means that the address is unique on that LAN but there is no guarantee that the address is not being used in another NIC in another LAN somewhere else in the world. The IEEE standard specifies the first three bytes of the MAC address as the vendor address component sometimes known as vendor block code. The IEEE standard calls the unique block code an organizationally unique identifier. The last three bytes of the MAC address is the serial number of that vendor's interface card, sometimes known as the vendor specific identifier. The IEEE standard assigns each vendor, that manufactures IEEE compliant NICs a unique three-byte block code. With three bytes, there are 2^{24} unique vendor block codes possible. Each vendor uses its vendor block code for the first three bytes of every NIC it manufactures. The last three bytes are vendor specific and should be different on every NIC sold by a vendor. With three bytes, there are 2^{24} hardware addresses assigned to each NIC vendor. The second bit (b_1) of the first byte of the MAC address is called the G/L bit (G = global and L = local). The address is globally unique, if $b_1 = 0$ and locally unique, if $b_1 = 1$.

Q.5. Explain binary exponential back-off algorithm. ***(R.G.P.V., Dec.***

Or

Discuss any one algorithm for allocating a multiple access cha ***(R.G.P.V., Dec.***

Ans. To ensure that random back-off maintains stability, CSMA/C a technique known as binary exponential back-off. ***Binary exponential off algorithm*** varies the limit on number of slot times. It works in the follo manner –

(i) If a station's frame collides for the first time, wait 0 or 1 slot (selected randomly) before trying again.

(ii) In case of colliding a second time, wait 0, 1, 2 or 3 slot (selected randomly).

(iii) If it collides third time, wait anywhere from 0 to 7 slots.

(iv) Generally, if there are n collisions, then wait anywhere 0 to $2^n - 1$ slots if n <= 10. If n > 10, wait between 0 and 2^{10} (1024)

(v) After 16 collisions, give up and report an error.

Thus, as congestion increases, stations back-off by larger and larger amounts to reduce the probability of collision. This method clearly attempts reduce excessive waits by keeping the number of possible time slots small After all if two stations collide, there is a 50% opportunity they will succeed on the next attempt (assuming that no other stations are transmitting).

If several stations collide, however, the opportunities are very small even one will be successful on next attempt. The successful one would have to select either 0 or 1 slot with all the others making the other selections raising the number of possible slots after every collision, the opportunities colliding again decrease exponentially.

Q.6. Explain the terms 'static channel allocation' and 'dynamic cha allocation'. ***(R.G.P.V., June***

Ans. **Static Channel Allocation** – The traditional method of allocating a single channel, such as a telephone trunk, among multiple competing is frequency division multiplexing (FDM). If the number of users is then the bandwidth is divided into N equal sized portions, every user located one portion. There is no interference between users because user has a private frequency band. If number of users are fixed and each of which has a heavy load of traffic, then FDM is a simple and allocation mechanism.

In case, if the number of senders are large and continuously varying traffic is bursty, FDM presents some problems. When the spectrum is into N regions and fewer than N users are currently interested

communicating, a large piece of valuable spectrum will be wasted. If more than N users have desire to communicate, few of them will be denied permission due to lack of bandwidth, even if some of the users who have been assigned a frequency band hardly ever send or receive anything.

However, even supposing that the number of users could somehow be held constant at N, dividing the single channel into static subchannels is inherently inefficient. The main difficulty is that when some users are quiescent, their bandwidth is simply lost. They are not using it and no one else is permitted to use it either. Furthermore, data traffic is too much bursty in most computer systems. In addition, most of the channels will be idle most of the time.

By using simple queueing theory, the poor performance of static FDM can be calculated. For a channel of capacity C bps, with an arrival rate of λ frames/sec, each frame having a length drawn from an exponential probability density function with mean $1/\mu$ bits/frame. The mean time delay T is given as –

$$T = \frac{1}{\mu C - \lambda}$$

Now, it is assumed that the single channel is divided into N independent subchannels, each with capacity C/N bps. Thus, the mean input rate on every subchannel will be λ/N. On recomputing T, it is obtained that –

$$T_{FDM} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT$$

Using FDM, the mean delay is N times worse than when all the frames were somehow magically arranged orderly in a big central queue.

The arguments which apply to FDM also apply to TDM. Every user is statically allocated every Nth time slot. If the allocated slot is not used by the user, it just lies fallow. Because none of the traditional static channel allocation schemes work well with bursty traffic, dynamic methods are used.

Dynamic Channel Allocation – In dynamic channel allocation schemes, following key assumptions are made –

(i) Station Model – There are N independent stations (computers, telephones etc.) in the model, each with a program or user which produces frames for transmission. The probability of a frame being produced in an interval of length Δt is $\lambda \Delta t$, where λ is a constant. Once a frame has been produced, the station is blocked and does nothing until the frame has been successfully transmitted.

(ii) Single Channel Assumption – There is a single channel for all communication. All stations can send on it and all can receive from it. In the hardware's point of view, all stations are equivalent, although protocol software may assign priorities to them.

(iii) Collision Assumption – When two frames are sent simultaneously they overlap in time and the resulting signal is garbled. This event is known as collision. Collisions can be detected by all stations. A collided frame must be sent again later. There are no errors other than those produced by collisions.

(iv) Continuous Time – At any instant, frame transmission can begin. There is no master clock dividing time into discrete intervals.

(v) Slotted Time – Discrete intervals of time are made. A frame will have 0, 1 or more frames, corresponding to an idle slot, a successful transmission or a collision respectively.

(vi) Carrier Sense – Stations can tell if the channel is in use before trying to use it. In the matter of sensing channel as busy, no station will make effort to use it until it goes idle.

(vii) No Carrier Sense – Before trying to use a channel, stations cannot sense. They just go ahead and send. Only later can they find out whether or not the transmission was successful.

Q.7. How is possible to allocate static channel in LANs and MA ***(R.G.P.V., June***

Ans. Refer the ans. of Q.6.

DISTRIBUTED RANDOM ACCESS SCHEMES/CONTENTI SCHEMES – FOR DATA SERVICES (ALOHA AND SLOTTE ALOHA), FOR LOCAL-AREA NETWORKS (CSMA, CSMA/ CSMA/CA)

Q.8. Write detailed note on ALOHA. (R.G.P.V., June 2007, Dec

Ans. In seventies, Norman Abramson and his colleagues at the Univ of Hawaii developed a new method to solve the channel allocation p This method was known as ALOHA system. It is used as ground-bas broadcasting. It is applicable to any shared transmission medium. Th idea is applicable to the system with multiple users competing for the single shared channel.

In the ALOHA scheme, each individual user transmits at any ti time when there is a message to be sent. If more than one user tries to at the same time, the message collide and have to be transmitted la scheme is the simplest possible because it is fully asynchronous, that is is no coordination among users. However, because there is a high-inte possibility between messages from different simultaneously transmitte the maximum obtainable channel utilization is only about 18 percent. T two versions of ALOHA – pure ALOHA and slotted ALOHA.

Q.9. What is the concept of pure ALOHA ? Also find its throughput ?
Or
Show that for about pure ALOHA, the maximum throughput is 1/2e and occurs at G = 0.5. ***(R.G.P.V., June 2005)***

Ans. In ALOHA system, uniform frame size is used. This increases the throughput of ALOHA system. With pure ALOHA, frames are transmitted at completely arbitrary times. In other words, the stations transmit whenever they have data to be sent. Whenever two frames try to occupy the channel at the same time, there will be a collision. Thus, both the frames will be garbled.

The simple working of pure ALOHA pays the penalty in terms of increased number of collisions with increased load. Thus the maximum utilization of the channel is only about 18 percent.

Basic idea of pure ALOHA is simple because users transmit immediately whenever they have data to send. For deciding whether a transmission was successful, a sender waits for an acknowledgement from the receiver for a time period equal to two propagation times $2t_{prop}$, that is, the time it takes a packet to travel from the sender to the receiver and back again. If acknowledgement is not received after this time, a back-off algorithm is used to choose a random retransmission time. The packet is dropped if acknowledgement is not received after k retransmission attempts. There are a number of ways to select the average back-off time.

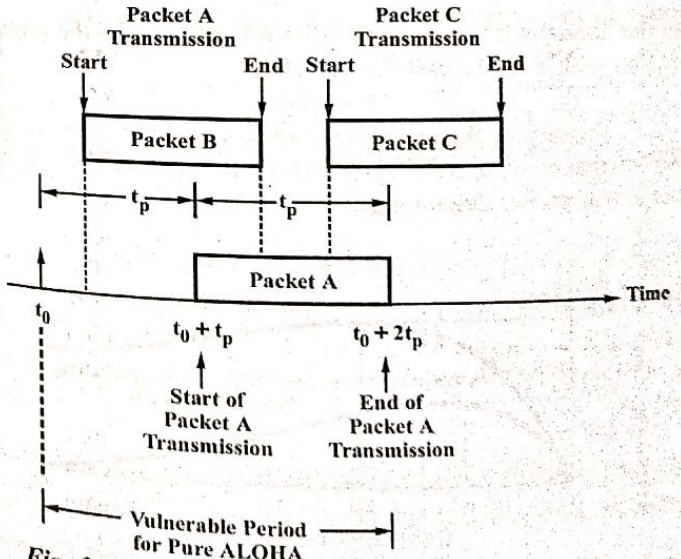


Fig. 3.2 Vulnerable Period during which Packets can Collide in the Pure ALOHA Method

As shown in fig. 3.2, there will be collisions between packets sent within a packet retransmission time t_p from different users. Firstly, it is assumed that

all packets have the same length and each needs one time unit t_p (known as slot) for transmission. Consider an effort made by a user to send packet A starting time $t_0 + t_p$ and ending at time $t_0 + 2t_p$. If packet B had been generating by another user between t_0 and $t_0 + t_p$, the end of the packet collide with the beginning of packet A. This can happen because, on long propagation delays, the sender of packet had no knowledge that B was already underway when the transmission of packet A was start the same way if another user makes an effort to transmit between $t_0 + t_p$ $t_0 + 2t_p$ (packet C), the starting of packet C will collide with the end of A. Therefore, as shown in fig. 3.2, if two packets overlap by even the small amount in the vulnerable period of length $2t_p$, both packets will be corrupted and will require to be transmitted later.

Assume that S is the channel throughput (the average number of successful transmissions per time period t_p) and G is the total traffic entering the channel from an infinite population of users (i.e., G represents the number of packet transmissions which are attempted in a time period t_p). To obtain the throughput firstly it is assumed that the probability p_k of k transmission attempts per packet time follows a Poission distribution with a mean G per packet time. Therefore, this probability is given as –

$$P_k = \frac{G^k e^{-G}}{k!}$$

Then the throughput S is just the offered load G times the probability of a transmission which is successful. Therefore –

$$S = G.p_0$$

where, p_0 = Probability that a packet does not suffer a collision (i.e., the probability that no other traffic is produced in the duration of a vulnerable period that is two packet times long).

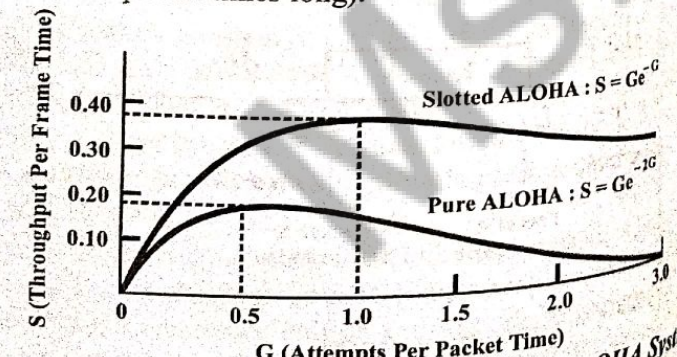


Fig. 3.3 Throughput versus Offered Load for ALOHA Systems

From equation (i), the probability of zero packets being produced in interval two packet times long is given as –

$$p_0 = e^{-2G}$$

From equation (iii), putting the value of p_0 in equation (ii) –

$$S = Ge^{-2G} \quad \ldots(iv)$$

Throughput given by equation (iv) is plotted in fig. 3.3. At G = 0.5, maximum value of S obtains where, $S = \frac{1}{(2e)}$ that is about 0.184. It means that the best channel utilization can be obtained is around 18 percent in the pure ALOHA method.

Q.10. What do you understand by slotted ALOHA ?

Ans. In 1972, Reberts gave a method for doubling the capacity of an ALOHA system. This method is called slotted ALOHA. This scheme divides the total time into discrete intervals. Each interval corresponds to one frame. A central or master clock is sent in order to achieve synchronization among all stations. Transmission of frame is permitted to begin at the start of next slot. This reduces the collisions and the maximum utilization of the system increases upto 37 percent.

Q.11. Consider the delay of pure ALOHA versus slotted ALOHA at the low load. Which one is less ? Explain your answer. (R.G.P.V., June 2016)

Ans. Pure ALOHA allows users to transmit whenever they have data to be sent. Like CSMA/CD collision can and do happen in such a scheme. At low load, no collisions are expected so the transmission is likely to be successful. In slotted ALOHA, the overall time is divided into several time slices or intervals. Each interval corresponds to one frame. Thus, the clock is tied to frame transmission. This means that a user cannot transmit data arbitrarily now. We need to wait for the next slot beginning time to transmit. The user can transmit only when the interval for the next frame starts. This approach mandates that all the users agree with the slot boundaries. This introduces half a slot time of delay.

Q.12. What is the effect of delay time in ALOHA on its throughput ? (R.G.P.V., Dec. 2017)

Ans. Refer the ans. of Q.11.

Q.13. What is the difference between slotted ALOHA and pure ALOHA ? (R.G.P.V., Dec. 2012)

Or

Compare the pure ALOHA and slotted ALOHA. (R.G.P.V., Dec. 2006, 2009)

Ans. Comparison between pure ALOHA and slotted ALOHA is given below –

S.No.	Pure ALOHA	Slotted ALOHA
(i)	In pure ALOHA, frames are transmitted at arbitrary times.	In slotted ALOHA, since time is divided up into discrete slots, the frame is sent at the start of a slot.

(ii)	The performance is given by $S = Ge^{-2G}$	The performance is given by $S = Ge^{-G}$
(iii)	The maximum utilization is about 18 per cent.	The utilization is double as pure ALOHA. It is about 37 pe
(iv)	It does not require global time.	It requires global time syn nization, as it is divided in discrete slots.
(v)	Due to very low utilization factor, it cannot be used for satellites.	It is used in broadcast satell
(vi)	Its implementation is very simple.	Its implementation is compara complex due to the synchroniz of all stations.

Q.14. Write a short note on ALOHA. Differentiate pure ALOHA slotted ALOHA. ***(R.G.P.V., June***

Ans. Refer the ans. of Q.8 and Q.13.

Q.15. Explain why S-ALOHA is better than pure ALOHA.
(R.G.P.V., May/June 2006, June

Or

Explain why the efficiency of pure ALOHA is half of slotted ALO
(R.G.P.V., June

Ans. For increasing the efficiency of the ALOHA method, the slotted AL method is introduced. In this scheme, channel is divided into time slots tha exactly equal to a packet transmission time. Then, all users are synchroniz these time slots so that if a user produces a packet, it must synchronize co with the next possible channel slot. Consequently, the vulnerable period in t this packet can collide with other data is minimized to one packet time p versus two for pure ALOHA. Fig. 3.4 shows examples of transmission att and random retransmission delays for colliding packets for four network s

Because the vulnerable period is now decreased to half, the probabil no other traffic occurring during the same time period as the packet wa to transmit is $p_0 = e^{-G}$. As a result, a throughput becomes as –

$$S = Ge^{-G}$$

At G = 1, the maximum efficiency for the slotted ALOHA syste obtained where, S = 1/e or about 0.368, which is twice that of pure AL

If the slotted ALOHA operates at G = 1, the probability of empty sl is 0.368. In the best performance of slotted ALOHA, 37% empty slots successful and 26% collisions occur. Operating slotted ALOHA at higher of G reduces the number of empty slots but increases the colli

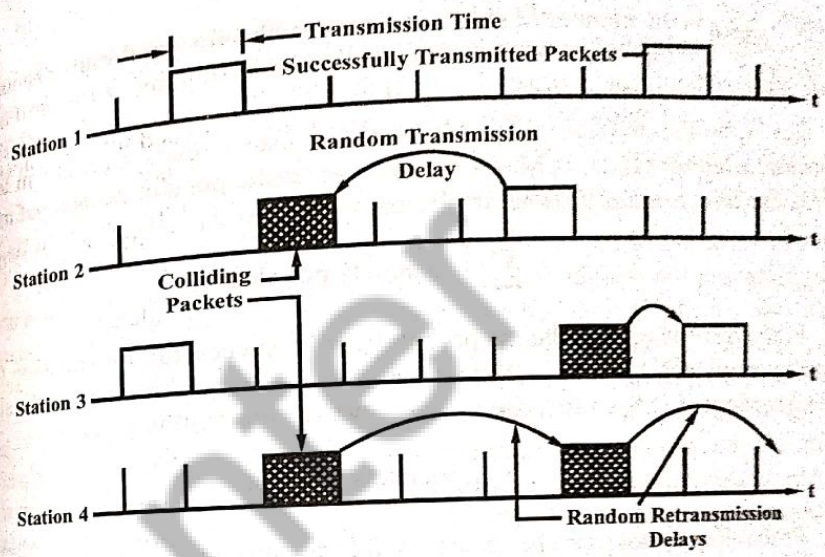


Fig. 3.4 Examples of Transmission Attempts and Random Retransmission Delays for Colliding Packets in Slotted ALOHA

exponentially and the overall performance goes down. Hence small increases in the channel load (users) can drastically reduce its performance.

This is the reason why S-ALOHA is better than pure ALOHA.

Q.16. Explain ALOHA and slotted ALOHA protocol. Compare the efficiency in each case. ***(R.G.P.V., Dec. 2014)***

Ans. Refer the ans. of Q.8, Q.10, Q.9, and Q.15.

Q.17. Derive an expression to prove that throughput of "slotted ALOHA" is approximately twice than that of "pure ALOHA". (R.G.P.V., Dec. 2017)

Ans. Refer the ans. of Q.9 and Q.15.

Q.18. Explain slotted ALOHA protocol. Derive efficiency for slotted ALOHA protocol. ***(R.G.P.V., June 2012)***

Ans. **Slotted ALOHA** – Refer the ans. of Q.10.

Let, there be a finite number of users in a slotted ALOHA system. For starting, first the relative-frequency concept of probability is examined so that for station i the steady-state average throughput S_i and the offered traffic G_i can be defined by the following expressions –

$$S_i = \frac{N_{i,\,good}}{N_T} = \text{Probability that station i successfully transmits}$$

$$G_i = \frac{N_{i,\,attempt}}{N_T} = \text{Probability that station i attempts transmission}$$

where $N_{i, good}$ is the number of slots used by station i for good transmi
$N_{i, attempt}$ is the number of slots in which station i attempts to trans
N_T is the total number of slots.

Let G_i be the probability for M users that user i sends a packet
given slot where i = 1, 2, …, M. As the average traffic per slot because o
i is G_i, the total average channel traffic is given as –

$$G = \sum_{i=1}^{M} G_i \text{ packets per slot}$$

In the same way, let S_i be the probability of a successful transmissio
a packet produced by user i. It means that the average throughput pe
because of user i is S_i so that the average total throughput is given as -

$$S = \sum_{i=1}^{M} S_i \text{ packets per slot}$$

Probability S_i that user i has a successful transmission in a particular
slot then is merely the probability G_i that the user i transmits a packet, multi
by the probability that none of the other M – 1 users transmit packets. Therefo

$$S_i = G_i \prod_{j \neq i} (1 - G_j)$$

Q.19. Write short note on CSMA. (R.G.P.V., Dec. 2003, Nov./Dec. 2

Or

Explain CSMA protocol in detail. ***(R.G.P.V., June 2***

Ans. With CSMA, a station wishing to transmit first listens to the medi
to determine if another transmission is in progress. If the medium is in use
station must wait. If the medium is idle, the station may transmit. It
happen that two or more stations attempt to transmit at about the same
If this happens, there will be a collision; the data from both transmissions
be garbled and not received successfully. To account for this, a station w
a reasonable amount of time after transmitting for an acknowledgement, tak
into account the maximum round trip propagation delay and the fact that
acknowledging station must also contend for the channel to respond. If
is no acknowledgement, the station assumes that a collision has occurred
retransmits.

One can see how this strategy would be effective for networks in wh
the average frame transmission time is much longer than the propagation
Collisions can occur only when more than one user begin transmitting w
short time. If a station begins to transmit a frame and there are no collis
during the time it takes for the leading edge of the packet to propagate
farthest station, then there will be no collision for this frame because all
stations are now aware of the transmission.

The ***maximum utilization*** achievable using CSMA can far exceed than that of ALOHA or slotted ALOHA.The maximum channel utilization depends on the length of the frame and on the propagation time; the longer the frames, or the shorter the propagation time, the higher the utilization.

Q.20. In p-persistent CSMA, the value of 'p' is wrongly estimated. How will it effect network performance ? ***(R.G.P.V., June 2003, Dec. 2008)***

Ans. In p-persistent CSMA difference from the other case is that stations do not transmit with 100% probability, but they include the probability factor p. p-persistent CSMA protocol applies to slotted channels here a station sense the channel before starting its transmission. If it find the channel idle, it either transmits the frame with probability p or defers until the next slot with probability q = 1 – p. If the next slot is also idle it either transmits or defer again, with probability p and q. This process is repeated again and again until the frame is transmitted. If the value of p is wrongly estimated in p-persistent CSMA then collision chances are increased. Consequently network performance are affected. Resulting network efficiency will be decreased.

Q.21. Explain 1-persistent, non-persistent and p-persistent CSMA. Compare them in terms of delay and efficiency. ***(R.G.P.V., Dec. 2004)***

Or

Explain 3 versions of CSMA protocol. ***(R.G.P.V., June 2008)***

Ans. With CSMA, three algorithms or approaches are used to specify what a station should do if the medium is found busy.

(i) 1-persistent CSMA – To avoid situations in which a station has to wait before transmitting even though the channel is idle, 1-persistent CSMA protocol is developed. The 1-persistent CSMA approach operates by transmitting a packet with probability 1, if the channel is sensed idle. When a station has to transmit a packet and channel is busy, station waits until the channel becomes idle and then transmits immediately with probability 1. This scheme is named "1-persistent" because station persists on transmitting when the channel is busy and then transmits its packet with probability 1. If two or more stations are waiting to transmit, a collision is guaranteed because every station will transmit immediately at the end of the busy period. In this case, every station will wait a random amount of time and then will reattempt to transmit.

In this protocol, the station wishing to transmit listens to the medium and obeys the following rules –

(a) If the medium is idle, transmit; otherwise, go to step (b).

(b) If the medium is busy, continuously listen until the channel is sensed idle then transmit immediately.

The protocol is called 1-persistent because the station transmits with a probability of 1 whenever it finds the channel idle.

Performance of 1-persistent CSMA protocol depends on the channel time. Assume just after a station starts transmitting, another station packet to send and checks to see if the channel is idle. In the condition packet from the first station has not yet arrived at the second station, the will assume the channel is idle and will transmit its packet, therefore cr a collision. As the delay time becomes longer, this effect becomes important because the performance of the protocol reduces.

The throughput of 1-persistent CSMA is written as –

$$S = \frac{Ge^{-G(1+2a)}[1+G+aG(1+G+aG/2)]}{G(1+2a)-(1-e^{-aG})+(1+aG)e^{-G(1+a)}}$$

(ii) Non-persistent CSMA – A station wishing to transmit listens the medium and obeys the following rules –

(a) If the medium is idle, transmit; go to step (b).

(b) If the medium is busy, wait an amount of time drawn from a probability distribution (the retransmission delay) and repeat step (a).

The use of random delays reduces the probability of collisions. This less greedy than 1-persistent CSMA. Intuitively this algorithm should lead better channel utilization and longer delays than 1-persistent CSMA.

$$S = \frac{Ge^{-aG}}{G(1+2a)+e^{-aG}}$$

(iii) p-persistent CSMA – The p-persistent CSMA scheme is developed to minimize the interference resulting from collisions and to increase the throughput. This is the general case of the 1-persistent CSMA protocol that is applied to slotted channels. In this protocol, if a station becomes ready to transmit and it senses the channel to be idle, it either sends with a probability p or defers transmission by one time slot with a probability $q = 1 - p$. When the deferred slot is also idle, the station either sends with a probability p defers again with a transmission probability q. Until the packet is transmitted or channel becomes busy, this process is repeated. The station acts as though there had been a collision if the channel becomes busy; that is, it waits random time and then begins the transmission attempt again. In case the channel originally was sensed to be busy, the station waits for the next slot and applies the preceding procedure.

A compromise that attempts to reduce collisions, like non-persistent reduce idle time, like 1-persistent is p-persistent. The rules are as follows –

(a) If the medium is idle, transmit with probability p and delay one time unit with probability $(1 - p)$. The time unit is typically equal to maximum propagation delay.

(b) If the medium is busy, continue to listen until the channel is idle and repeat step (a).

(c) If the transmission is delayed one time unit, repeat step (a).

A comparison between various protocols is shown in fig. 3.5.

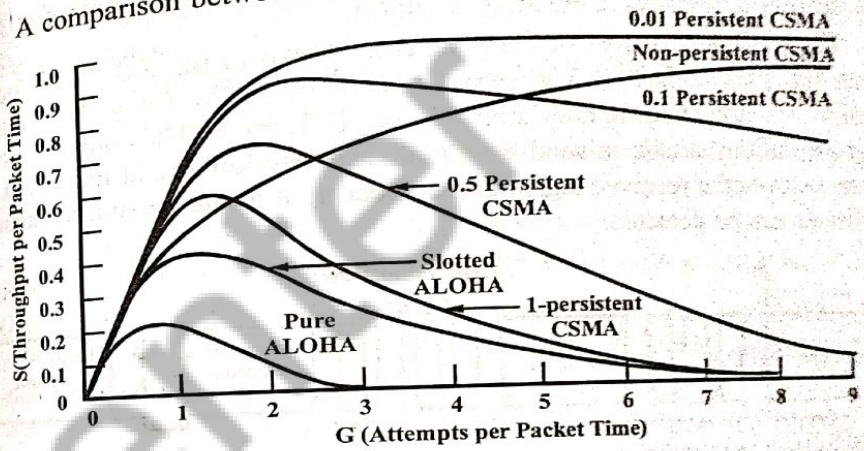


Fig. 3.5 Comparison of Channel Utilization vs Load for Various CSMA Protocols and ALOHA

Q.22. How can you compare 1-persistent CSMA and p-persistent CSMA ? ***(R.G.P.V., June 2011, Dec. 2016)***

Or

Differentiate between 1-persistent CSMA and p-persistent CSMA protocols. ***(R.G.P.V., June 2015)***

Ans. Refer the ans. of Q.21.

Q.23. What is channelization ? Define time division multiple access. ***(R.G.P.V., June 2015)***

Ans. Channelization is a multiple access scheme in which the available link bandwidth is shared in time, frequency, or through code, between various stations. There are three channelization protocols as follows –

(i) Frequency division multiple access (FDMA)

(ii) Time division multiple access (TDMA)

(iii) Code division multiple access (CDMA).

Time Division Multiple Access – In TDMA, the stations share the channel bandwidth in time. Each station is assigned a time slot during which it may transmit data. Each station sends its data in is allocated time slot.

Q.24. What is CSMA/CD ? Explain.

Ans. When two stations sense the channel to be idle and start transmitting simultaneously, they will both detect the collision almost at once. Rather than

finish transmitting their frames, that are irretrievably garbled anyway, should abruptly stop transmitting as soon as collision is detected. Time bandwidth are saved by rapidly terminating damaged frames. This protocol called ***CSMA/CD*** (***carrier sense multiple access with collision detection***) is widely used on LANs in the MAC sublayer.

The conceptual model of CSMA/CD is shown in fig. 3.6. At the point marked t_0, a station has finished transmitting its frame. Now any other station having a frame to transmit may attempt to do so. There will be collision if two or more stations decide to send simultaneously. By looking at the power pulse width of the received signal and comparing it to the transmitted signal, collisions can be detected.

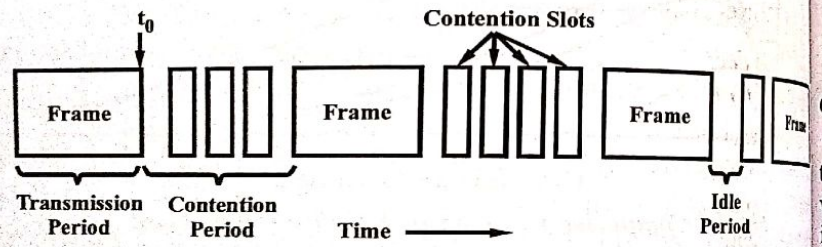


Fig. 3.6 Three States of CSMA/CD (Contention, Transmission or Idle)

When a station detects a collision, it absorbs its transmission, waits a random period of time and then attempts again, assuming that no other station has started sending in the meantime. Thus, CSMA/CD model will have alternating contention and transmission periods with idle periods occurring when all stations are quiet.

To see the details of the contention algorithm, suppose that two stations both start transmitting at exactly time t_0. The time, required to realize a collision is determined by the length of the contention period and hence what the delay and throughput will be. Then, the minimum time to detect the collision is just the time it takes the signal to propagate from one station to another.

The important thing to be realized is that collision detection is an analog process. At the time of transmitting, station's hardware must listen to the cable. If what it reads back is different from what it is putting out, it knows a collision is occurring. Implication is that signal encoding must permit collisions to be detected. Due to this reason, special encoding is commonly used.

Q.25. Make a comparison between pure ALOHA, slotted ALOHA and CSMA/CD. ***(R.G.P.V., May 20...***

Ans. Refer the ans. of Q.13 and Q.24.

Q.26. Give the advantages and disadvantages of IEEE 802.3 (CSMA/CD).

Ans. **Advantages** – Some advantages of IEEE 802.3 are as follows –

(i) This protocol is simple and is widely used.
(ii) Stations can be easily installed without affecting the network.
(iii) A passive cable is used and modems are not required.
(iv) The delay at low load is practically zero and so the stations can transmit immediately.

Disadvantages – Some disadvantages of IEEE 802.3 are given below –

(i) There is no priority scheme for the frames to send.
(ii) This protocol provides no acknowledgements, thus leading to unreliability.
(iii) Not suited to real-time applications.
(iv) Gives poor performance at high load.

Q.27. How does CSMA/CD protocol improve the performance over CSMA protocol for long frames ? ***(R.G.P.V., Dec. 2015, June 2017)***

Ans. Whenever multiple users have unregulated access to a single line, there is a danger of signals overlapping and destroying each other. Such overlaps, which turn the signals into unusable noise, are called *collisions*. As traffic increases on a multiple access link, so do collision. A LAN therefore needs a mechanism to coordinate traffic, minimize the number of collisions that occur, and maximize the number of frames that are delivered successfully. The access mechanisms used in an Ethernet is ***called carrier sense multiple access with collision detection (CSMA/CD)***.

CSMA/CD is the result of an evolution from multiple access (MA) to carrier sense multiple access (CSMA) and finally to carrier sense multiple access with collision detection. The original design was a multiple access method in which every workstation had equal access to link. In MA, there was no provision for traffic coordination. Access to the line was open to any node at any time, with the assumption that the odds of two devices competing for access at the same time, were small enough to be unimportant. Any station wishing to transmit did so, then relied on acknowledgments to verify that the transmitted frame had not been destroyed by other traffic on the line.

In a CSMA system any workstation wishing to transmit must first listen for existing traffic on the line.

A device listens by checking for a voltage. If no voltage is detected, the line is considered idle and the transmission is initiated. CSMA cuts down on the number of collisions but does not eliminate them. Collision can still occur. If another station has transmitted too recently for its signal to have reached the listening station the listener assumes the line is idle and introduces its own signal onto the line.

The final step is the addition of collision detection (CD). In CSMA/CD, the station wishing to transmit first listens to make certain the link is free, then

transmit its data, then listens again. During the data transmission, the ... checks the line for the extremely high voltages that indicate a collis... collision is detected, the station quits the current transmission and ... predetermined amount of time for line to clear, than send its again.

Q.28. What is need of minimum frame size ? *(R.G.P.V., Jun...*

Ans. We need a restriction on the frame size for CSMA/CD ... Before transmitting the last bit of the frame, the sending station must ... collision, if any, and stop the transmission. This is so because the ... once the entire frame is sent, does not keep a copy of the frame and ... monitor the line for collision detection.

The minimum length restriction is required for the correct operat... CSMA/CD. An Ethernet frame needs to have a minimum length of 64 ...

Q.29. Write brief note on CSMA/CA (carrier sense multiple acces... collision avoidance).

Ans. The wired network, in which the received signal has almos... same energy as the transmitted signal, since either the length of the ca... short or there are repeaters which amplify the energy between the transm... and the receiver. It means that in a collision, the detected energy almost doub... But, in a wireless network, much of the transmitted energy is lo... transmission. The received signal contains very little energy. Thus, a colli... may add only 5 to 10 percent additional energy, which is not useful for effe... collision detection.

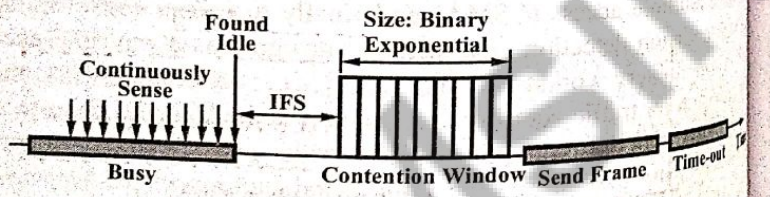


Fig. 3.7 Timing in CSMA/CA

Avoidance of collisions on wireless networks is required, becaus... cannot be detected. ***Carrier sense multiple access with collision avoid... (CSMA/CA)*** was invented for this network. By CSMA/CA collisions are a... through the use of three strategies –

(i) Interframe Space (IFS) – When the channel is found id... station does not transmit immediately, it waits for a time period know... interframe space (IFS). Although the channel may appear idle when it is ... a distant station may have already started transmitting. The distant s... signal has not yet reached this station. The IFS time permits the front ... transmitted signal by the distant station to reach this station. When afte... IFS time the channel is still idle, the station can transmit, but it still ...

wait a time equal to the contention time. The IFS variable is also used to prioritize stations or frame types. A station which is located a shorter IFS has a higher priority.

(ii) Contention Window – It is an amount of time divided into slots. A channel which is ready to transmit, selects a random number of slots as its wait time. The station requires to sense the channel after each time slots. If the station finds the channel is busy, it does not restart the process, it just stops the timer and restarts it when the channel is sensed as idle. This provides priority to the station with the longest waiting time.

(iii) Acknowledgements – The acknowledgements guarantee that the receiver has received the frame.

Q.30. Explain CSMA and protocols with collision detection and avoidance. ***(R.G.P.V., May 2019)***

Ans. Refer the ans. of Q.19, Q.24 and Q.29.

Q.31. Draw the flowchart for CSMA/CD and CSMA/CA procedure and explain in detail. ***(R.G.P.V., June 2010)***

Ans. **Flow Diagram Process for CSMA/CD** – The flow diagram for CSMA/CD is shown in fig. 3.8. It has some differences with the ALOHA protocol, otherwise we can say it is similar to the ALOHA protocol.

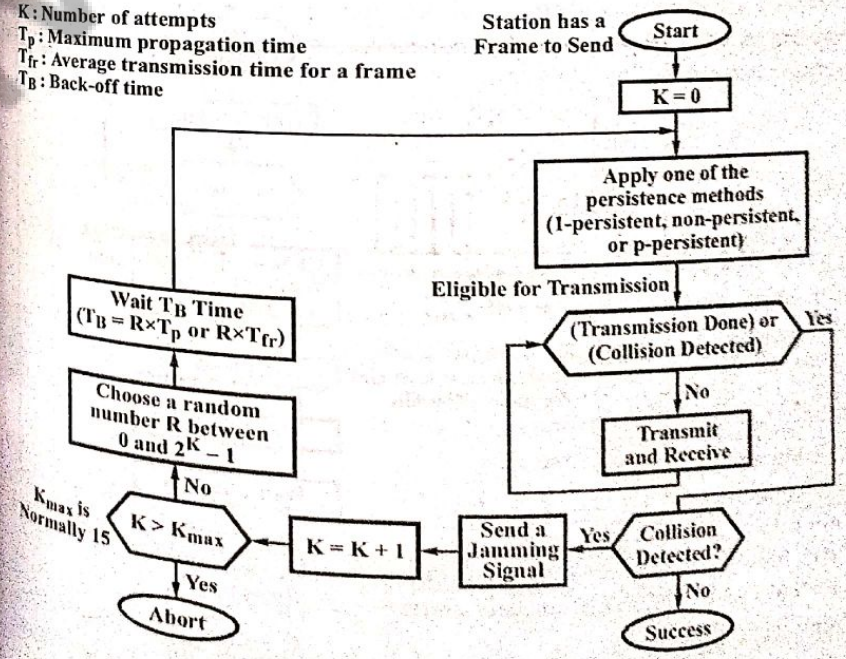


Fig. 3.8 Flow Diagram for CSMA/CD

The first difference is the frame transmission. In ALOHA, we s the entire frame and then wait for an acknowledgement. On the other CSMA/CD, transmission and collision detection is a continuous pro do not transmit the entire frame and then look for a collision. The sends and receives continuously and simultaneously. We use a loop to s that transmission is a continuous process. We constantly monitor i one of two conditions – either transmission is finished or a collision is When we come out of the loop, if a collision has not been detected, that transmission is complete, the entire frame is transmitted. Othe collision has occurred.

The second difference is the sending of a short jamming signal enforces the collision in case other stations have not yet sensed the co

The third difference is the addition of the persistence process. We to sense the channel before we start sending the frame by using one persistence processes.

Flow Diagram Process for CSMA/CA – Fig. 3.9 shows the flow di for CSMA/CA.

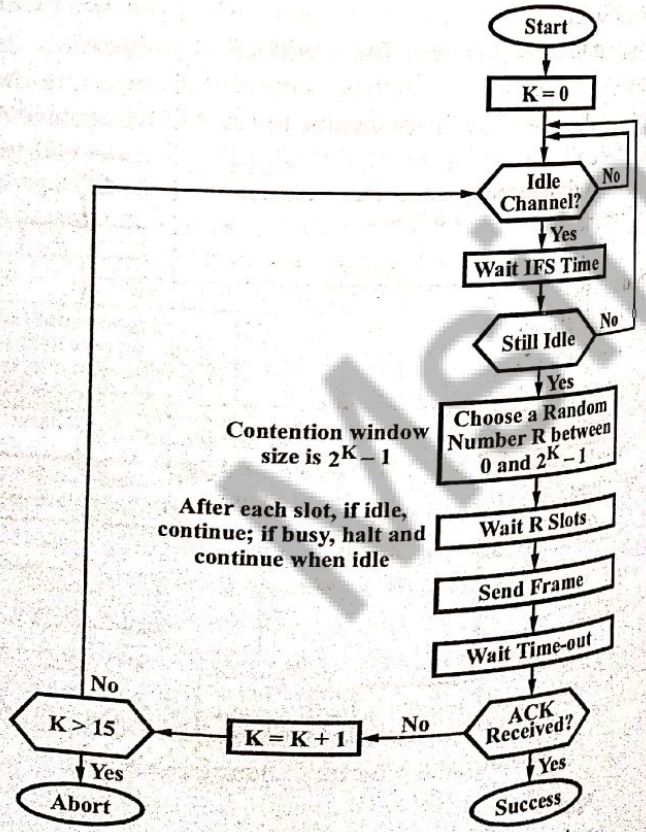


Fig. 3.9 Flow Diagram for CSMA/CA

Here, the channel requires to be sensed before and after the IFS. During the contention time, the channel also requires to be sensed. The channel is sensed for each time slot of the contention window. If it is found idle, the timer continues, if the channel is found busy, the timer is stopped and continues after the timer becomes idle again.

Q.32. Compare CSMA, CSMA/CD and CSMA/CA techniques used in MAC layer. ***(R.G.P.V., Dec. 2010)***

Or

How does CSMA/CD differ from CSMA/CA ? ***(R.G.P.V., Dec. 2012)***

Ans. The comparison among CSMA, CSMA/CD and CSMA/CA are given below –

S. No.	CSMA	CSMA/CD	CSMA/CA
(i)	It employs the concept of "sense before transmitting".	It also employs the concept of "sense before transmitting".	It also employs the concept of "sense before transmitting".
(ii)	It is used with LANs configured in a bus topology.	It is used in wired LANs as a MAC method.	It is used with wireless LANs.
(iii)	It reduces the likelihood of a collision. However, it does not eliminate the possibility, and it does not provide procedures to deal with them when they occur.	It is same as CSMA except that it includes procedures to detect collisions and deal with them when they occur.	It is same as CSMA/CD except CSMA/CA implements steps to prevent collisions from occuring.
(iv)	A station continues transmission of a frame until the end of the frame even if a collision occurs.	If a station is transmitting and a collision is detected then tramsmission of the wasted frame is abandoned.	We need to avoid collisions on wireless networks because they cannot be detected. Collisions are avoided through the use of CSMA/CA's three strategies the interframe space, the contention window, and acknowledgements.

NUMERICAL PROBLEMS

Prob. 1. Suppose a group of N stations share a 56 kbps pure ALOHA channel. Each station outputs 1000 bit frame on an average of once every

100 sec. even if the previous one has not yet been sent (e.g. the station buffer outgoing frames). What is the maximum value of N ?

(R.G.P.V., Dec. 2014,

Sol. In case of pure ALOHA, the usable bandwidth

$= 0.184 \times 56$ kpbs $= 10.3$ kbps $= 10300$ bps

Because every station needs 10 bps, thus

$$N = \frac{10300}{10} = \mathbf{1030\ stations}$$

Prob.2. Ten thousand airline reservation stations are competing for use of a single slotted ALOHA channel. The average station makes 18 requests hour. A slot is 125 μsec. What is the approximate total channel load?

(R.G.P.V., June 20

Sol. In every 200 sec, every terminal makes one request for a total load of 50 requests/sec.

$$\therefore \quad \text{Total channel load } G = \frac{50}{8000} = \frac{\mathbf{1}}{\mathbf{160}}$$

Prob.3. A large population of ALOHA users manages to generate request/sec, including both originals and retransmissions. Time is slotted unit of 40 msec.

(i) What is the chance of success on the first attempt ?
(ii) What is the probability of exactly K collisions and then a succes
(iii) What is expected number of transmission attempts needed
(iv) What is throughput of channel ?

(R.G.P.V., June 20

Sol. The time is slotted in unit of 40 msec. This time is called avera transmission time T_{fr} for a frame. Thus

$T_{fr} = 40$ msec

$T_p = 50$ request/seconds

(i) When there is no other traffic during the same slot the chance of success on the first attempt is e^{-G}. With $G = 2$, the poisson gives a probability of e^{-2}.

(ii) The probability of a transmission requiring exactly K collis followed by one success is

$$P_K = e^{-G}(1 - e^{-G})^K = 0.135 \times 0.865^K$$

(iii) The expected number of transmissions E, per carriage typed is then

$$E = \sum_{1}^{\infty} KP_K = \sum_{K=1}^{\infty} Ke^{-G}(1 - e^{-G})^{K-1} = e^{G}$$

i.e.

$$e^2 = 7.3890$$

(iv) Throughput of channel is given by $S = Ge^{-G} = 2 \times e^{-2}$

$= 0.270$ i.e. 27% only

Prob.4. A large population of ALOHA users manage to generate 50 request/sec including both originals and retransmissions. Time is slotted in units of 40 msec.

(i) What is the chance of success in the first attempt ?
(ii) What is the probability of exactly K collisions and then success ?

(R.G.P.V., May 2018)

Sol. Refer the sol. of Prob.3.

Prob.5. Define the throughput of pure ALOHA ? A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kpbs. What is the throughput if the system (all stations together) produces –

(i) 1000 frames per second (ii) 500 frames per second
(iii) 250 frames per second.

(R.G.P.V., June 2015)

Sol. Refer the ans. of Q.9.

First, we calculate

$$\text{Frame transmission time} = \frac{200 \text{ bit}}{200 \text{ kbps}} = 1 \text{ m sec}$$

(i) If the system produces 1000 frames per second, this is 1 frame per m sec.

The load G is 1. In this case, the throughput is given by

$$S = G \times e^{-2G}$$
$$= 1 \times e^{-2\times1} = 0.135 = 13.5\%$$

This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

(ii) If system produces 500 frames per second, this is $\left(\frac{1}{2}\right)$ frame per m sec $\left(\frac{500}{1000} = \frac{1}{2}\right)$, i.e.

$$G = \frac{1}{2}$$

Throughput, $S = G \times e^{-2G} = \frac{1}{2} \times e^{-2\times1/2} = 0.184 = 18.4\%$

This means that the throughput is $500 \times 0.184 = 92$ frames. Only 92 frames out of 500 will probably survive.

(iii) If system produces 250 frames per second, this is $\left(\frac{1}{4}\right)$ frame per m sec $\left(\frac{250}{1000} = \frac{1}{4}\right)$, i.e.

MSRUVerter

$$G = \frac{1}{4}$$

Throughput, $S = G \times e^{-2G} = \frac{1}{4} \times e^{-2\times\frac{1}{4}} = 0.152 = 15.2\%$

This means that the throughput is $250 \times 0.152 = 38$ frames. Out frames out of 250 will probably survive.

Prob.6. Consider a slotted ALOHA having five stations. If the offered load $G_1 = 0.1$, $G_2 = 0.15$, $G_3 = 0.2$, $G_4 = 0.25$ and $G_5 = 0.3$ packets, find individual throughput of each station and channel throughput. *(R.G.P.V., June 20*

Sol. For finite population, slotted ALOHA

$$S_i = G_i e^{-G_i}$$

where i = (1 to M) for M stations

G_i = The probability that station i transmits a packet in any given

= Offered load by station i

S_i = Probability of a successful transmission for a packet gener by user i (i.e., t)

Also $$S = \sum_{i=1}^{M} S_i$$

where S is the total throughput.

Given, $i = 1$ to 5

$G_1 = 0.1$, $G_2 = 0.15$, $G_3 = 0.2$, $G_4 = 0.25$, $G_5 =$

Then,

$S_1 = G_1 e^{-G_1} = 0.1\, e^{-0.1} = 0.0905$

$S_2 = G_2 e^{-G_2} = 0.15\, e^{-0.15} = 0.1291$

$S_3 = G_3 e^{-G_3} = 0.2\, e^{-0.2} = 0.1637$

$S_4 = G_4 e^{-G_4} = 0.25\, e^{-0.25} = 0.1947$

$S_5 = G_5 e^{-G_5} = 0.3\, e^{-0.3} = 0.2222$

Individual throughputs,

$S_1 = \mathbf{0.0905 \times 100 = 9.05\%}$

$S_2 = \mathbf{0.1291 \times 100 = 12.91\%}$

$S_3 = \mathbf{0.1637 \times 100 = 16.37\%}$

$S_4 = \mathbf{0.1947 \times 100 = 19.47\%}$

$S_5 = \mathbf{0.2222 \times 100 = 22.22\%}$

Total (channel) throughput,

$S = S_1 + S_2 + S_3 + S_4 + S_5$

$= 0.0905 + 0.1291 + 0.1637 + 0.1947 + 0.$

$= \mathbf{0.8002}$

Prob.7. Sketch the Manchester encoding on a classic ethernet for the bit stream 0001110101. *(R.G.P.V., Dec. 2015)*

Sol. The Manchester encoding is shown in fig. 3.10.

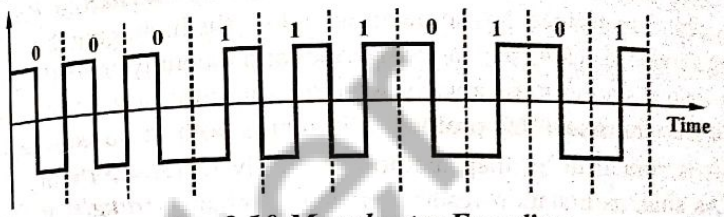


Fig. 3.10 Manchester Encoding

COLLISION FREE PROTOCOLS – BASIC BIT MAP, BRAP, BINARY COUNT DOWN, MLMA, LIMITED CONTENTION PROTOCOLS – ADAPTIVE TREE WALK

Q.33. What are the various collision free protocols ? Explain.

Ans. The collisions can be completely avoided if we adopt this type of protocol. There is a reservation procedure adopted in each of the case. The station that reserves the channel first get the chance to transmit first. Some of the important protocols of this variety are –

(i) Bit Map Protocol – In this variety, the total contention period is divided into as many slots as there are number of stations. Now each station has a number and thus aware of its position in the subdivided contention interval. Whenever a previous transmission ends, contention period begins and all the stations those who want to transmit, transmit a bit in their respective slot period. The situation for a 8 station bit map protocol is shown below and during the reservation period stations 1, 3 and 7 reserve. They are then allowed to send their respective order as if every other stations are aware of their reservation. They do not interfere and transmission is thorough.

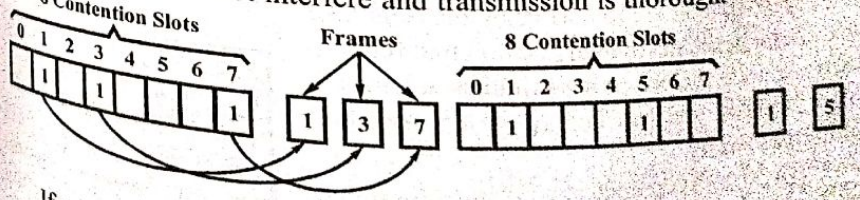


Fig. 3.11

If we try to find the degree of channel utilization then it is different at low and high load. Whenever the load is low, i.e., out of a group of N stations only single station wishes to transmit its frame of d bits, the overhead here is of N bits resulting in a channel utilization of d/(N + d). On the other hand, at high

load when all the stations wish to transmit, the N bit contention period o... is distributed over N frames resulting in a overhead of only 1-bit per fra... an efficiency of d/(d + 1).

(ii) BRAP (Broadcast Recognition with Alternating Priori...

The basic bit map protocol has some drawbacks – the higher numbered st... get better service than lowered numbered ones and secondly under the cond... of light load a station must always wait for the current scan to be fi... before it may transmit. This protocol eliminates both these drawbacks.

This is similar to bit map method, the only difference being as sh... below. As soon as a station reserves it gets a chance to send the mess... After its transmission is over the next station gets a chance to reserve, a... this case the waiting time after reservation is absent. After every station h... once been given a chance to reserve, the cycle repeats. Here the delay tim... dependent on the difference of number between the current station and t... station lost successfully transmitted model N.

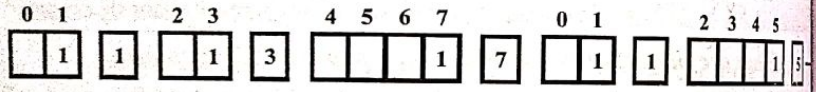


Fig. 3.12

The channel efficiency of BRAP is identical to the basic bit map meth... its delay characteristics are better.

(iii) Binary Countdown – In this type of method, there is a address... methodology. Each station has a address (unique) and that too in equal numb... of bits, i.e., if there are 64 stations then each may be assigned a unique bina... address of $\log_2 64 = 6$ bits. During the reservation process, each station b... transmits the most significant address bit. When all have done so the n... MSB is transmitted and so on. Every time all the MSB's transmitted by differ... station are Boolean-ORed and stored in a buffer. While transmitting th... respective bits each station takes care that if already there is a higher addr... station in the contest they immediately give up transmission paving a way... the higher address station. Thus by the time LSB transmission arrives the only station that remains in the arena is the one with the highest address. It then transmits its data and again a reservation procedure starts.

The fig. 3.13 here indicates the situation among 4-stations who wish to transmit among a group of 16. First all the stations transmit their MSB's (bit at time 0). These MSB's are Boolean-ORed to get the result (1 here). Now the stations who have transmitted 0 as MSB (0010 and – 0100).

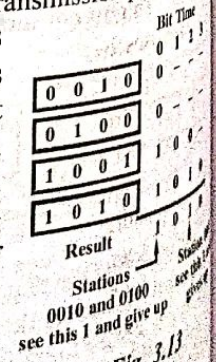


Fig. 3.13

See that there are higher numbered stations competing by seeing the result 1 and so give up. Next the stations 1001 and 1010 transmit their next bit. The bits are ORed and the process continues. When both the station transmit their third bit and they are ORed the result comes out to be 1; seeing it the station 1001 give up finally by the time LSB is transmitted only 1010 remains and this station is given a chance to transmit its data, after which another cycle starts. The efficiency here is given as $\frac{d}{d + \log_2 N}$. The disadvantage is that the higher order address station gets a preference.

Q.34. Explain the MLMA LAN protocol.

Ans. MLMA (Multi-Level Multi-Access Protocol) is a method that is very efficient under conditions of high channel load but has a shorter delay under conditions of low channel load. In this method, a station announces that it wants to send by broadcasting its address in a particular format. The idea behind it is illustrated by means of an example using radix 10 arithmetic and N = 1000. An address in this system consists of three decimal digits, each decimal digit represented by a group of 10 bits called a "decade". For example, 472 is represented by setting bit 4 in the first decade, bit 7 in the middle decade, and bit 2 in the last decade.

If only one station attempts to transmit during a frame slot, it uses the 30 bit header to announce itself and then it sends its frame. The trouble arises when two or more stations try to insert their addresses into the same header. To disambiguate all of the addresses, the stations behave as follows. The first decade in every frame slot corresponds to the hundreds place in the station number. After the first decade is finished, stations that have not transmitted a bit must remain silent until all the stations that did set a bit have transmitted their data. Call the highest occupied bit position in the first decade x. In the second decade, all stations with x as their leading digit announce their ten's place. Call the highest occupied bit here y. In the third decade, all the stations whose addresses begin with xy may set the bit corresponding to their last digits. There are atmost 10 of them.

Fig. 3.14 explains this example for five stations, with addresses 122, 125, 705, 722 and 725. Here, x = 7 and y = 2. After decade 2, all stations now know that 722 and 725 want to send, and that furthermore one or more stations with addresses between 700 and 709, and one or more stations with addresses between 100 and 199 also want to send. Decade three identifies 705. Decade four is used for the ten's place of all stations in the highest "century" not yet fully identified. In this case, the 100 series stations get to broadcast their tens places next. If station 342 had also set its bit in decade 0, decade 4 would have been devoted to the 300 series stations instead of the 100

series. After the 100 series stations have broadcast their tens places, ev... knows that the highest (and only) remaining group of stations is 120-1... the following decade is used to separate them out. Finally, the data are ... numerical order of the station addresses.

Bit Position	9	8	7	6	5	4	3	2	1	0	
	0	0	1	0	0	0	0	0	1	0	Decade 0 (122, 125, 705, 722, ...
	0	0	0	0	0	0	0	1	0	1	Decade 1 (705, 722, 725 Send)
	0	0	0	0	1	0	0	1	0	0	Decade 2 (722, 725 Send)
	0	0	0	0	1	0	0	0	0	0	Decade 3 (705 Send)
	0	0	0	0	0	0	0	1	0	0	Decade 4 (122, 125 Send)
	0	0	0	0	1	0	0	1	0	0	Decade 5 (122, 125 Send)

Fig. 3.14 MLMA, The Recognition of Stations 122, 125, 705, 722, a... 725 Requires 60 Bits

The number of decades needed to resolve conflicts depends on ... addresses themselves. To separate 122 and 129 requires only three decad... but to separate 122 and 229 requires five decades. If all 1000 stations wa... send, decade 0 is 0-999, decade 1 is for the 900 series, decade 2 is for 9... 999, decade 3 is for 980-989 and so on. Decade 10 is for 900-909, decade ... is for the ten's place of the 800 series stations, and so forth. In all, 111 decad... are needed for the header (the initial one, the 10 "centuries", and the ... decades that differentiate on the ones place).

The channel efficiency is difficult to calculate exactly, but for a mini... channel load, 30 bits of header are needed, giving an efficiency of d/(d+30)... the limit of a very heavy load, a frame consists of 111 decades of header and ... data frames, for an efficiency of d/(d + 1.11) which is close to the efficiency ... the bit-map method. The mean delay under conditions of light load is just 2 ...

It is clear that the choice of radix 10 was an arbitrary choice. Any ... radix would do, also. To minimize the number of bits in the header for the ... of only one request per frame, consider some radix r with l levels ("decade... The number of levels for a given r is the smallest value of l such that l ... We seek to minimize the number of bits in the header, l_r, subject to the constr... $r^l \geq N$. The minimum occurs at r = e. For 1000 stations, $r = 2$ and l = ... best, but for 2000 stations the optimum radix is 3, with seven levels.

Q.35. What do you mean by limited contention protocol ? Explain any one. (R.G.P.V., June 2012)

Ans. The combination of the best properties of the contention and collision-free protocols provides a new protocol that uses contention at low load to provide low delay and a collision free technique at high load to provide good channel efficiency. Such protocols are called as limited-contention protocols. One such protocol is discussed below –

Adaptive Tree Walk Protocol – We can easily understand the adaptive tree walk protocol if we consider the stations as the leaves of a binary tree, as shown in fig. 3.15. In the first contention slot following a successful frame transmission, slot 0, all stations are allowed to try to get the channel. It is fine if one of them acquires the channel. If there is a collision, then during slot 1, only those stations falling under node B in the tree, may compete. If one of them acquires the channel, the slot following the frame is reserved for those stations which are under node C. On the other hand, if two or more stations, which are under node B, want to transmit, there will be a collision during slot 1, in which case it is node D's turn during slot B.

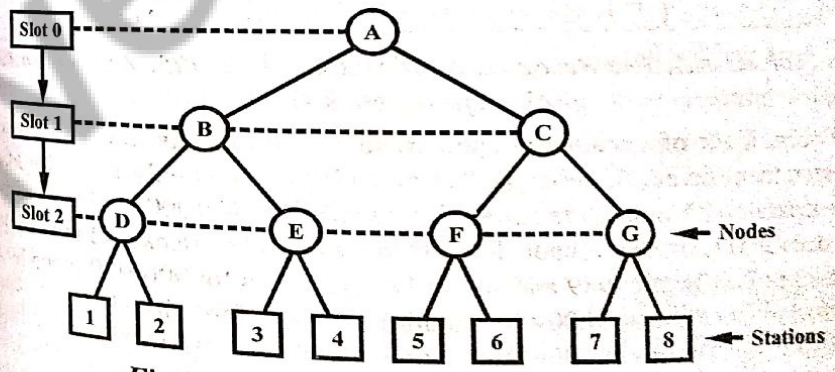


Fig. 3.15 Adaptive Tree Walk for 8-stations

In short, if a collision takes place during slot 0, the whole tree is searched, depth first, to locate all ready stations. Each bit slot is associated with certain nodes in the tree. The search continues recursively with the left and right children of node when a collision takes place. If a bit slot is found to be idle or if only one station wants to transmit in it, the searching of its node can stop because all ready stations have been located.

If the load on the system is heavy, it is hardly worm the effort to dedicate slot 0 to node A, since that makes sense only in the unlikely event which precisely one station has a frame to transmit. In similar way, one could argue that node B and C should be skipped as well for the same reason. Clearly, the heavier the load, the farther down the tree the search should again.

Q.36. How adaptive tree walk protocol works ? ***(R.G.P.V., June***

Ans. Refer the ans. of Q.35.

Q.37. Discuss adaptive tree walk and turn protocol in detail. ***(R.G.P.V., Dec.***

Ans. **Adaptive Tree Walk** – Refer the ans. of Q.35.

Turn Protocol – Traversal using relay NAT (TURN) is another NAT approach that uses the TCP/UDP pinhole opened through the NAT to establish a bidirectional communication tunnel with a TURN server in the network. The device D is located in the private network, which needs to a communication with the public Internet, first communicates with the server employing the TURN protocol. First, device D requests an IP and port for his own use on the TURN server. The TURN server allocates address and port (IP_t : port_t). Then, device D can advertise this IP and port to external IP devices that need to send packets to it. When the server receives packets on IP_t : port_t, it simply forwards these packets device D employing the TURN protocol. The TURN protocol can traverse NAT function because it is based on a permanent TCP connection between device D and the TURN server, or it uses symmetric UDP.

Q.38. Compare collision, collision free and limited contention sublayer protocol with suitable examples.(R.G.P.V., June 2014, Dec.

Ans. Collision protocols use carrier sensing as the means to resolve contention in the MAC sublayer. When multiple stations compete for access to a single channel they use CSMA or CSMA/CD approach to resolve the same. If a station can sense the carrier it can always find out whether transmission is going on or not and hence can decide when to transmit so that it can avoid a collision. However as many of the stations are of carrier sensing nature they all observe the carrier simultaneously as a result whenever the channel get freed (previous transmission ends) they all try to transmit, and collide with each other. Still there is an improvement over the ALOHA system.

(i) ALOHA – Refer the ans. of Q.8.

(ii) CSMA – Refer the ans. of Q.19.

Refer the ans. of Q.33 and Q.35.

Q.39. What is the difference between Multiple Access and (Collision Avoidance (MACA) and MACAW (for wireless) ? ***(R.G.P.V., June***

Ans. In MACA, the sender stimulate the receiver into outputting a frame, so other stations can detect this transmission and avoid transmitting for the duration of the upcoming (large) data frame. Fig. 3.16 shows multiple access with collision avoidance. To send a frame C to D, C sends Request To Send (RTS) frame to D. This 30 byte frame has the length of

data frame that will eventually follow. Thereafter, D sends a Clear To Send (CTS) frame. The CTS frame has the data length copied from the RTS frame. C begins transmission after receiving the CTS frame from D.

On the basis of simulation studies of MACA, Bharghavan fine tuned MACA to enhance it performance and renamed it MACAW. To start with, they noticed that without data link layer acknowledgements, lost frames were not retransmitted until the transport layer noticed their absence, much later. This problem is solved by using an ACK frame after each successful data frame. They observed the need of CSMA to keep a station from transmitting an RTS at the same time another nearby station is also doing so to the same destination. Besides, they decided to run the backoff algorithm separately for each data stream instead of each station. Thus, the performance of the protocol improves. At last, for improving system performance they add a mechanism for stations to exchange information about congestion and a way to make the backoff algorithm react less violently to temporary problems.

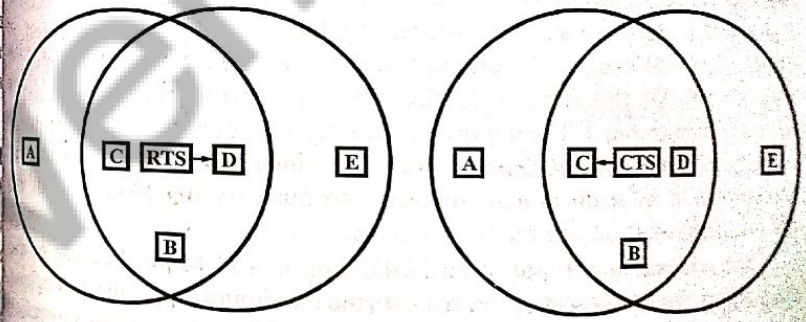


Fig. 3.16 MACA Protocol

Q.40. Explain URN protocol. ***(R.G.P.V., June 2015)***

Ans. A uniform resource name (URN) protocol is an Internet resource with a name that, unlike a URL has persistent significance (i.e. the owner of the URN can expect that someone else will always be able to find the resource). A frequent problem in using the Web is that Web content is sometimes moved to a new site or a new page on the same site. Since links are made using uniform resource locators (URLs), they no longer work when content is moved. For example,

urn : def : // blue_laser

Where "def : // might represent an agency or an accessible directory of all dictionaries, glossaries, and encyclopedias on the Internet and "blue laser" was the name of a term. A comparable URL would require to specify one specific location for a definition such as : http : // www.what is.com / blue laser htm. For this case, the user has to know where the resource is assigned as well as how to spell the file name and suffix. With a URN, the user only

requires to know the name of a resources. One or more agencies will pro... be able to locate the nearest copy of the resource. The user is free... understanding where resources are assigned or reassigned to.

Both URN and URL are types of a concept known as uniform ... identifier (URI). A URN can be associated with another concept ... uniform resource characteristics (URC), which permits descriptive info... to be associated with a URN, like, author, date, length, and so forth.

PERFORMANCE MEASURING METRICS, IEEE STANDARD 802 SERIES & THEIR VARIANT

Q.41. What are the performance measuring metric for a com... network ? Define each of them. *(R.G.P.V., May ...*

Ans. The two important performance measures associated with ... medium networks are maximum obtainable throughput and the mean ... access delay. Both are strongly influenced by the MAC algorithm ... share the available transmission capacity between the attached stations. ... case of an FDDI, this is based on the use of a control token and the ... token rotation protocol. The important parameter associated with the pro... is the target token rotation time (TTRT) and, since this must be presen... same value in all stations, it is important to quantify its effect on bo... obtainable throughput and the access delay.

The nominal throughput of an FDDI ring is 100 Mpbs, because ... ring latency and access control mechanism, the maximum obtainable throu... is less than this. Maximum obtained throughput (and access delay) ... that there are always frames waiting to be sent on receipt of the token a... ring interface. The access delay is defined as the time delay betwe... arrival of a frame at the ring interface of the source station and its deliv... the ring interface at the destination station. Therefore, the access delay in... any time spent waiting in the ring interface queue at the source until a ... (early) token arrives. It is meaningful only if the offered load is less tha... maximum obtainable throughput of the ring, otherwise the interface q... continuously build up and the access delay gets progressively larger.

Q.42. Explain IEEE 802 standards for LAN. *(R.G.P.V., Jun...*

Ans. The various standards of IEEE 802 are as follows –

(i) 802.1 – The high level interface standard addresses ma... related to network architecture, interconnection and management. M... it deals with issues related to the higher OSI layers.

(ii) 802.2 – Logical link control (LLC) and media access control ... are two sublayers within 802.2 that are equivalent of the OSI data link la...

(iii) 802.3 – Carrier sense multiple access with collision detection (CSMA/CD) standards cover a variety of architectures that are generally based on the Ethernet as originally proposed by Metcalfe and Boggs.

(iv) 802.4 – The token bus network standard describes how the token bus network operates.

(v) 802.5 – The token ring network standard describes how the token ring network operates.

(vi) 802.6 – The metropolitan area network (MAN) standard describes the operation of network covering bigger distances. Another MAN standard, the distributed queue dual bus (DQDB) by the ANSI is an adoption of the IEEE MAN standard.

(vii) 802.7 – The broadband Technical Advisory Group provides guidance to other groups that are involved in establishing broadband LAN standards.

(viii) 802.8 – The Fibre Optic Technical Advisory Group provides guidance to other groups that are involved in establishing LAN standards using fibre optic cable.

(ix) 802.9 – Integrated data and voice networks standards cover the architecture for networks that carry both voice and data like ISDNs.

(x) 802.10 – A LAN security addresses the implementation of security capability like encryption /decryption network management and data transfer.

(xi) 802.11 – The wireless LAN standard covers multiple transmission methods for wireless transmission.

(xii) 802.12 – The demand priority access method is one of the newer groups which are involved in developing specifications for 100 Mbps speed over twisted-pair wires.

(xiii) 802.14 – Cable TV based broadband communication network working group.

(xiv) 802.15 – Wireless personal area network (WPAN) working group.

(xv) 802.16 – Broadband wireless access (BBWA) working group.

(xvi) 802.17 – Resilient packet ring working group (RPRWG) for use in LAN, MAN and WAN for transfer of data packets at rates scalable to many Gbps.

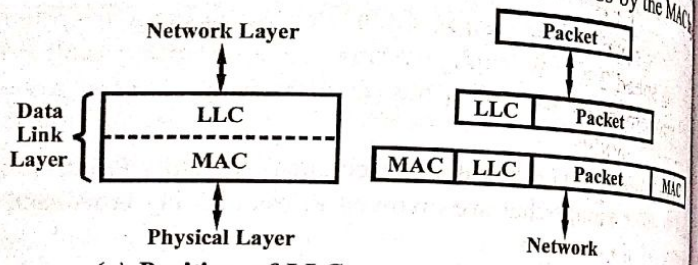
Q.43. Explain IEEE 802.2 in detail. *(R.G.P.V., June 2017)*

Ans. IEEE 802.2 has been defined by IEEE as an error-controlled, flow-controlled data link protocol. LLC can run on top of all the 802 LAN and MAN

protocols. In addition, this protocol called ***LLC (logical link control)*** the differences between the various types of 802 networks by pro single format and interface to the network layer. LLC forms the upper the data link layer, with the MAC layer below it (see fig. 3.17). LLC characteristics not shared by most other link control protocols –

(i) It must support the multiaccess shared-medium nature of

(ii) It is relieved of some details of link access by the MAC



(a) Position of LLC *(b) Protocol Formats*

Fig. 3.17

The network layer on the sending machine passes a packet to LLC the LLC access primitives. The LLC sublayer then adds an LLC h containing sequence and acknowledgement numbers. The resulting str is then inserted into the payload field of an 802.X frame and transmitt the receiver, the reverse process takes place.

LLC provides three service options –

(i) Unreliable datagram service

(ii) Acknowledged datagram service

(iii) Reliable connection-oriented service.

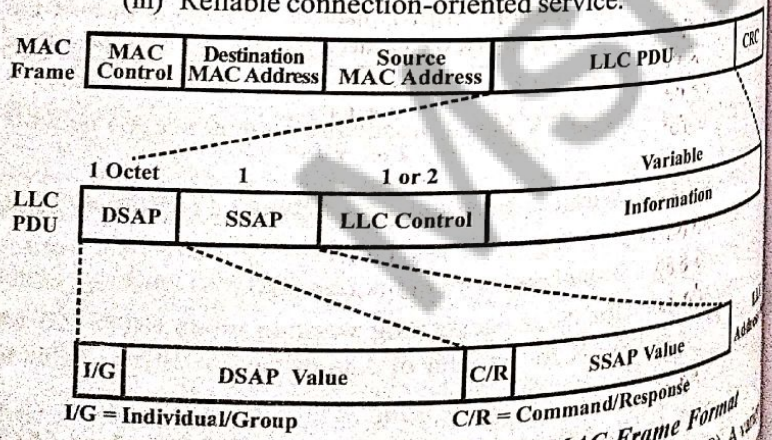


Fig. 3.18 LLC PDU in a Generic MAC Frame Format

The LLC header is based on HDLC protocol (see fig. 3.18). A va different formats are used for data and control. For acknowledged

or connection-oriented service, the data frames contain a source address, a destination address, a sequence number, an acknowledgement number and a few miscellaneous bits. For unreliable datagram service, the sequence number and acknowledgement number are omitted.

Q.44. Write a short note on Ethernet (IEEE 802.3).

(R.G.P.V., May/June 2006)

Ans. The Ethernet was developed by Xerox corporation in 1976. It was originally developed for connecting about 100 terminals with nearly 1 km cable having speed 2.94 Mbps. It was further upgraded to 10 Mbps. Ethernet was an improvement over earlier networks as it provided ways to manage the line when many stations tried to transmit on one wire (or cable) simultaneously. Ethernet uses carrier sensing for data transmission. It is based on the multiple access protocol 1-persistent CSMA/CD (carrier sense multiple access with collision detection).

In this category of LAN, if a station wants to transmit data, it listens to the cable. If the cable is busy, the station waits until it goes idle. If the cable is free, the data is transmitted immediately. If two or more stations want to transmit at the same time, both the stations sense each other's presence. Both then cease transmission, wait a random number of milliseconds and transmit again. The collision problem is thus solved. But Ethernet systems do not provide acknowledgements.

IEEE 802.3 standard defines two categories – ***baseband*** and ***broadband***, as shown in fig. 3.19. The word ***base*** specifies a digital signal (Manchester encoding). The word ***broad*** specifies an analog signal (PSK encoding). Five standards are defined for digital and one for analog category.

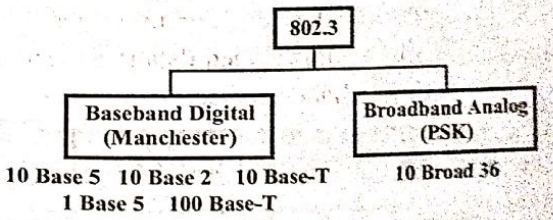


Fig. 3.19 IEEE 802.3

Baseband transmission implies that data is transmitted without the use of a carrier and with only one channel defined in the system. While in broadband transmission, there are multiple channels divided upto into different frequency bands. The broadband signalling supports the concurrent transmission of voice, data and video.

Q.45. What are the different line coding techniques ? Which is used in 802.3 LAN ?

(R.G.P.V., June 2014)

Ans. Table 3.1 lists some encoding techniques for representative LAN types.

Table 3.1

LAN Type	*Encoding Technique*
10 Base-T (Ethernet)	Manchester
100 Base-T (Fast Ethernet)	4B/5B, NRZ-I (optical fibre); MLT-3
Gigabit Ethernet	8B/10B (optical fiber); 4D-PAM5 (UT
4/10-Mbps token ring	Differential manchester
FDDI	4B/5B, NRZ-I (optical fibre); MLT-3
Fiber channel	8B/10B
Wireless LANs	BPSK, QPSK, QAM

Also, refer the ans. of Q.44.

Q.46. Give the frame format of IEEE 802.3 and explain various fi *(R.G.P.V., June*

Or

Describe the frame format of IEEE 802.3 standard for MAC subl *(R.G.P.V., Dec.*

Or

Explain the MAC frame format. *(R.G.P.V., June*

Ans. IEEE 802.3 specifies one type of frame having seven fi preamble, SFD, DA, SA, length/type of PDU, 802.2 frame and the C Ethernet has no mechanism for acknowledging received frames, maki what is known as an unreliable medium. Acknowledgments must implemented at the higher layers. Fig. 3.20 shows the format of the M frame is CSMA/CD.

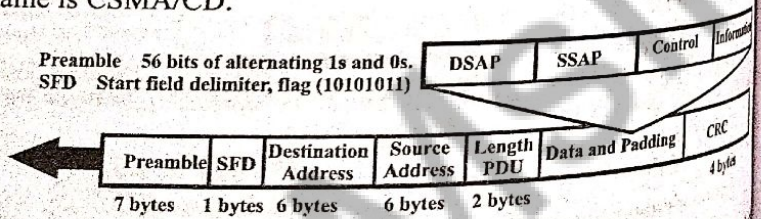


Fig. 3.20 802.3 MAC Frame

(i) Preamble – Preamble is the first field of 802.3 frame w contains seven bytes (7 × 8 = 56 bits) of altering 0s and 1s that ale receiving system to the coming frame and enable it to synchronize its timing. Pattern 1010101 provides only an alert and a timing pulse. It ca very easily aliased to be useful in indicating the starting of the data sta HDLC combined the alert, timing, and start synchronization into a singl – the flag. IEEE 802.3 divides these three frames between the preamble start frame delimiter (SFD) which the second field.

(ii) Start Frame Delimiter (SFD) – It is a one-octet field that marks the end of the preamble and beginning of the frame. The SFD field warns the station or stations that this is the last chance for synchronization. This field is identical to a preamble byte, except it ends with two 1s. Reception of SFD sequence indicates that the next byte is the destination address.

(iii) Destination Address (DA) – Destination address (DA) field contains six bytes and has the physical address of the packet's next destination. Physical address of a system is a bit pattern encoded on its network interface card (NIC). Each NIC contains a unique address which distinguishes it from any other NIC. If packet must cross from one LAN to another to reach its destination, the DA field has the physical address of the router connecting the current LAN to the next one. If the packet reaches the target network, then DA field has the physical address of the destination device.

(iv) Source Address (SA) – Source address (SA) field is allotted six bytes. It contains the physical address of the last device to forward the packet. That device can be the sending station for the most recent router to receive and forward the packet.

(v) Length/Type of PDU – These next two bytes tell the number of bytes in the coming PDU. When the length of the PDU is fixed, this field can be used to show type, or as a base for other protocols.

(vi) 802.2 Frame (PDU) – This field of the 802.3 frame has the entire 802.2 frame as a modulator, removable unit. Depending on the type of frame and the length of the information field, PDU can be any where from 46 to 1500 bytes long. PDU is produced by the upper (LLC) sublayer, then linked to the 802.3 frame.

(vii) Cyclic Redundancy Check (CRC) – This field is a four octet field that carries a CRC-32 error detection code derived from the header and data fields.

Q.47. Write a detailed note on token bus.

Ans. The standard 802.4 describes a LAN which is known as ***token bus***. Physically, the token bus is a linear or tree-shaped cable onto that stations are attached (see fig. 3.21). Logically, stations are organized into a ring with each station knowing the address of the station to its "right" and "left". If the logical ring is initialized, then highest numbered station may transmit the first frame. After it is done, it passes permission to its closest neighbour by transmitting the neighbour a special control frame known as a ***token***. The token propagates around the logical ring, with only token holder being allowed to send frames. Collisions do not occur because only one station at a time holds the token.

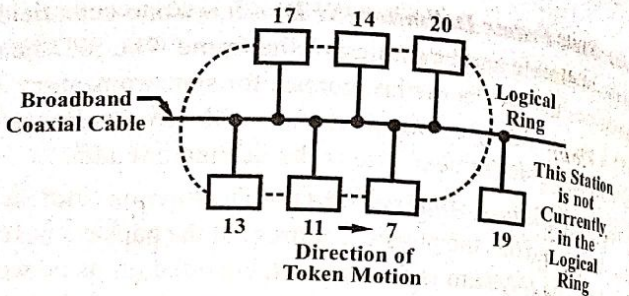


Fig. 3.21 Token Bus

The important thing to realize is that the physical order in which stations are connected to the cable is not important. Because the cable is inherently a broadcast medium, every station receives every frame, discarding those not addressed to it. If a station passes the token, then it transmits a token frame specifically addressed to its logical neighbour in the ring irrespective to the physical location of that station on the cable. It is also important to be noted that when stations are first powered on, they will not be in the ring. Therefore, the MAC protocol has provisions for adding stations and deleting stations from, the ring.

Q.48. Give advantages and disadvantages of token bus (IEEE 802.4).

Ans. **Advantages** – Advantages of token bus are as follows –

(i) It uses highly reliable cable television equipment.

(ii) It can handle short minimum frames.

(iii) It is more deterministic than 802.3 and so suitable for real time applications.

(iv) It supports priorities among the frames to send.

(v) The throughput and efficiency are excellent at high load.

(vi) Broadband cable can support multiple channels, not only for data, but also for voice and television.

Disadvantages – Disadvantages of token bus are as follows –

(i) This protocol is extremely complex and requires more hardware like modems and wideband amplifiers.

(ii) It has a small installed base of users.

(iii) It is poorly suited for fibre optic implementations.

(iv) It gives delay at low load.

Q.49. What happens in a token bus if a station accepts the token and then crashes immediately ? How does the protocol handles this situation ?

Ans. In a token bus, if a station accepts the token and crashes immediately then this problem can be solved using the ring initialization algorithm. Each station has a timer that is reset whenever a frame appears on the network.

When this timer hits a threshold value, the station issues a claim-token frame, and the modified binary countdown algorithm with random bits determines who get the token.

Q.50. Explain the frame format of IEEE 802.4 (token bus) protocol.
(R.G.P.V., May 2018)

Ans. The token bus frame format is shown in fig. 3.22. It is different from 802.3 frame format. For synchronizing the receiver's clock, ***preamble*** is used. ***Starting delimiter*** and ***ending delimiter*** are used for making the frame boundaries. Both of these fields have analog encoding of symbols other than 0s and 1s, therefore they cannot occur accidently in the user data. Due to this reason, no length field is required.

To distinguish data frames from control frame, ***frame control*** field is used. For data frames, it carries the priority of frame. It can also carry an indicator needing the destination station to acknowledge correct or incorrect receipt of the frame. Without this indicator, the destination would not be permitted to transmit anything because it does not contain the token. The token bus is turned by this indicator into something resembling the acknowledgement scheme of Tokoro and Tamaru.

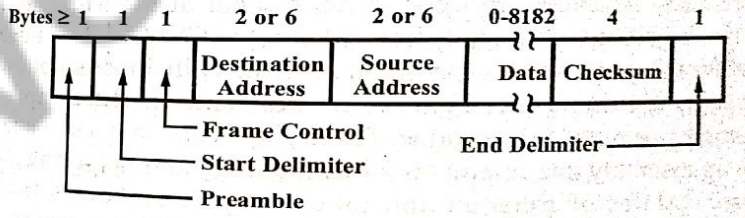


Fig. 3.22 802.4 Frame Format

Frame control field is used to specify the frame type for control frames. The permitted types include token passing and various ring maintenance frames, including the mechanism for letting new stations enter the ring, the mechanism for permitting stations to leave the ring and so on. It should be noted that the 802.3 protocol does not contain any control frames. All that the MAC layer does there is to provide a manner to get frames onto the cable. It does not care what is in them.

Destination address and ***source address*** fields are the same as in 802.3. As in the case of 802.3, a given network must use all 2 byte addresses or all 6 byte addresses, not a mixture on the same cable. The initial 802.4 standard permits either size. Individual and group addressing and the local and global address assignments are same as to 802.3.

Data field may be upto 8182 bytes long if 2 byte addresses are used and upto 8174 bytes long if 6 byte addresses are used. This is more than five times as long as the maximum 802.3 frame, that was made short to stop one station from hogging the channel too long. The timers can be used as an antilog

measure with the token bus but it is nice to be able to transmit long fr... when real-time traffic is not an issue. The **checksum** is used for dete... transmission errors. It uses the identical algorithm and polynomial as fo...

Q.51. What conditions would have to hold for a corrupted fram... circulate forever on a token ring without a monitor ? How does the mon... fix this problem ?

(R.G.P.V., June 20...

Ans. For a corrupted frame to circulate forever on a token ring with... monitor, the sender might either have failed or the frame's source address m... be corrupted so the sender does not recognize it. Persistently circulating fra... are detected by the monitor bit of the access control field. A monitor sta... fixes this by setting the monitor bit on the first pass. Frame with this bit no... its second pass are removed. The source address does not matter at this po...

Q.52. Explain why token bus is suited for real time application i... comparison to CSMA/CD with the help of suitable example.

(R.G.P.V., June 2008, Dec. 20...

Ans. Local area networks have a direct application in factory automati... and process control, where the nodes are computers controlling th... manufacturing process. In this type of application, real-time processing wi... minimum delay is needed. Processing must occur at the same speed as th... objects moving along the assembly line. Ethernet or CSMA/CD is not a suitab... protocol for this purpose because the number of collisions is not predictab... and the delay in sending data from the control center to the computers alo... the assembly line is not a fixed value. Token ring is also not a suitable protoc... because an assembly line resembles a bus topology and not a ring. Token bu... combines features of Ethernet and token ring. It combines the physic... configuration of Ethernet (a bus topology) and the collision-free (predictab... delay) feature of token ring. Token bus is a physical bus that operates as ... logical ring using tokens.

Stations are logically organized into a ring. A token is passed among statio... If a station wants to send data, it must wait and capture the token. However... like CSMA/CD stations communicate via common bus.

Token bus is thus limited to factory automation and process control a... has no commercial application in data communication.

Q.53. Compare IEEE 802.3, 802.4 and 802.5.

(R.G.P.V., May/June 2006, Dec. 20...

Or

(R.G.P.V., Dec. 20...

Compare the token bus and token ring.

Or

Differentiate between 802.3, 802.4 and 802.5 IEEE standards.

(R.G.P.V., June 2012, Dec. 20...

Ans. Comparison of Ethernet, Token Bus and Token Ring are as follows:

S.No.	Ethernet (802.3)	Token Bus (802.4)	Token Ring (802.5)
(i)	This is far and away the most widely used type at present, with a huge installed base and considerable operational experience. Stations can be installed on the fly without taking the network down.	It uses highly reliable cable television equipment.	It uses point-to-point connections.
(ii)	It is non-deterministic which is often inappropriate for real time work.	It is more deterministic than 802.3.	It is also deterministic.
(iii)	It has no priorities.	Token bus supports priorities and can be configured to provide a guaranteed fraction of the bandwidth to high-priority traffic such as digitized voice.	Similar to token bus, priorities are possible, although the scheme is not as fair.
(iv)	At high load, the presence of collisions becomes a major problem and can seriously affect the throughput.	It has excellent throughput and efficiency at high load.	Throughput and efficiency at high load are excellent.
(v)	Delay at low load is practically zero (stations do not have to wait for a token; they just transmit immediately).	It has substantial delay at low load (stations must always wait for the token, even in an otherwise idle system).	There is always delay at low load because the sender must wait for the token.
(vi)	It has a substantial analog component. Modems are not required.	It uses a lot of analog engineering and includes modems and wideband amplifiers.	It can be fully digital.
(vii)	Due to the possibility of having frames aborted by collisions, the minimum valid frame is 64 bytes.	It can handle short minimum frames.	Like the token bus, short frames are possible.

MSRuet

Q.54. Explain the functioning of wireless LAN in detail. **(R.G.P.V., May**

Ans. A wireless LAN is one that makes use of a wireless transmi medium. WLAN is a fast growing market introducing the flexibility of wir access into office, home, or production environments. WLANs are typi restricted in their diameter to buildings, a campus single room etc., and operated by individuals, not by large-scale providers. The main goal of WLA is to replace office cabling and, additionally to introduce a higher flexibility ad-hoc communication. Until relatively recently, wireless LANs were u used. The reasons for this included high prices, low data rates, occupatio safety concerns, and licensing requirements. As these problems have be addressed, the popularity of wireless LANs has grown rapidly.

The IEEE 802.11 committee developed a set of wireless LAN standard The model developed by the 802.11 working group is shown in fig. 3.23. basic service set (BSS) is the smallest building block of a wireless LAN. A BSS consists of some number of stations executing the same MAC protoco and competing for access to the same shared medium. A basic service set ma connect to a backbone distribution system through an access point, or may b isolated. The access point works as a bridge. The MAC protocol may b either fully distributed or controlled by a central coordination function housed in the access point. The BSS corresponds to what is called as a cell in the literature.

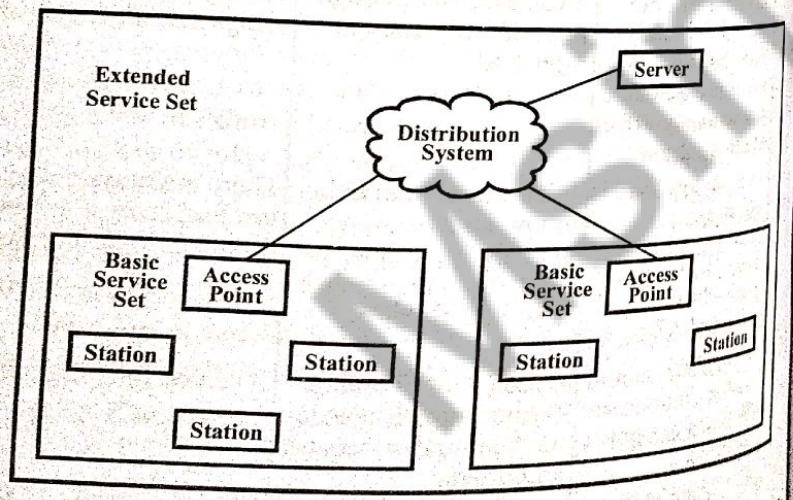


Fig. 3.23 IEEE 802.11 Architecture

An extended service set (ESS) comprises of two or more BSS interconnected by a distribution system. The distribution system is a wired backbone LAN. The ESS appears as a single logical LAN to the logical link control (LLC) level.

On the basis of mobility, the standard defined three kinds of stations –

(i) ***No-transition*** – This type of station is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.

(ii) ***BSS-transition*** – This type is defined as a station movement from one BSS to another BSS within the same ESS. In this situation, delivery of data to the station needs that the addressing capability be able to recognize the new location of the station.

(iii) ***ESS-transition*** – This type is defined as a station movement from a BSS in one ESS to a BSS within another ESS. This case is supported only in the sense that the station can move. There is no guarantee of maintenance of upper-layer connections supported by 802.11. In fact, disruption of service is likely to happen.

Q.55. Discuss Bluetooth architecture and its applications. **(R.G.P.V., Dec. 2010)**

Or

Write short note on Bluetooth. **(R.G.P.V., June 2013)**

Ans. In 1994, the L.M. Ericsson Company became interested in connecting its mobile phones to other devices (e.g., PDAs) without cables. Four other companies (IBM, Intel, Nokia and Toshiba), formed a SIG (special interest group, i.e., consortium) to develop a wireless standard for interconnecting computing, communication devices, and accessories using short-range, low-power, inexpensive wireless radios. The project was named ***Bluetooth***, after Harald Blaatand (Bluetooth) II (940-981), a Viking king who unified (i.e., conquered) Denmark and Norway, also without cables.

Although the original idea was just to get rid of the cables between devices, it soon began to expand in scope and encroach on the area of wireless LANs. While this move makes the standard more useful, it also creates some competition for mindshare with 802.11. To make matters worse, the two systems also interfere with each other electrically. It is also worth noting that Hewlett-Packard introduced an infrared network for connecting computer peripherals without wires some years ago, but it never really caught on in a big way.

The main goal of Bluetooth developing a single-chip, low-cost, radio-based wireless network technology.

At the same time the Bluetooth development started, a study group within IEEE 802.11 wireless personal area network (WPAN) discussed under the following five criteria –

(i) ***Distinct Identity*** – Originally the study group did not want to establish a second 802.11 standard.

(ii) Compatibility – Compatibility with IEEE 802 standard.

(iii) Market Potential – How many applications, devices, vend... customers are available for a certain technology ?

(iv) Technical Feasibility – Prototypes are necessary for ... discussion, so the study group would not rely on paper work.

(v) Economic Feasibility – Everything developed within this g... should be cheaper than other solutions and allow for high-volume produc...

Bluetooth fulfills these criteria so the WPAN group cooperated with th... Bluetooth consortium.

To understand the networking of Bluetooth devices a quick introduct... to its key features is necessary.

Piconet is the basic unit of Bluetooth system. Piconet consists of a mas... node and up to seven active slave nodes within a distance of 10 metres. Multip... piconets can exist in the same (large) room and can even be connected throug... a bridge node as illustrated in fig. 3.24. A Scatternet is defined as ... interconnected collection of piconets is.

There can be upto 255 parked nodes in the net for the seven active slav... nodes in a piconet. These are devices which the master has switched to a low... power state to minimize the drain on their batteries. In parked state, a devic... cannot do anything except respond to an activation or beacon signal from th... master. There are also two intermediate power states, hold and sniff.

The reason for the master/slave design is that the designers intended t... facilitate the implementation of complete Bluetooth chips for under $5. The... consequence of this decision is that the slaves are fairly dumb, basically ju... doing whatever the master tells them to do. Thus, a piconet is a centralize... TDM system, with the master controlling the clock and determining which... device gets to communicate in which time slot. All communication is betwe... the master and a slave; direct slave-slave communication is not possible.

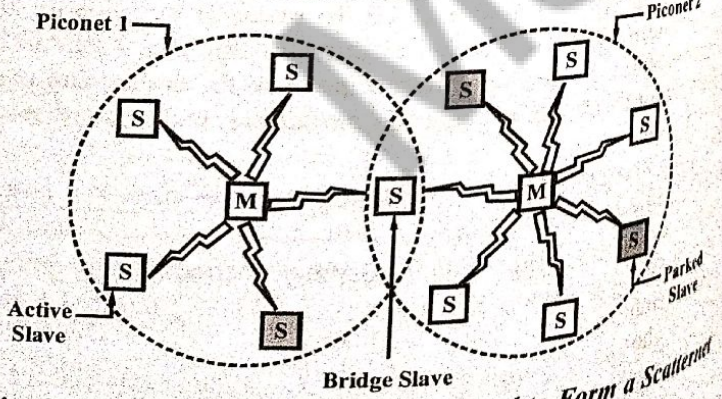


Fig. 3.24 Two Piconets can be Connected to Form a Scatternet

Applications – 802.11 does not specify whether users should use their notebook computers for reading e-mail, surfing the web, or something else. In contrast, the Bluetooth VI.I specification names 13 specific applications to be supported and provides different protocol stacks for each one. Unfortunately, this approach leads to a very large amount of complexity, which we will omit here. The 13 applications, which are called ***profiles***, are listed in fig. 3.25.

Name	*Description*
Generic access	Procedures for link management
Service discovery	Protocol for discovering offered services
Serial port	Replacement for a serial port cable
Generic object exchange	Defines client-server relationship for object movement
LAN access	Protocol between a mobile computer and a fixed LAN
Dial-up networking	Allows a notebook computer to call via a mobile phone
Fax	Allows a mobile fax machine to talk to a mobile phone
Cordless telephony	Connects a handset and its local base station
Intercom	Digital walkie-talkie
Headset	Allows hands-free voice communication
Object push	Provides a way to exchange simple objects
File transfer	Provides a more general file transfer facility
Synchronization	Permits a PDA to synchronize with another computer

Fig. 3.25 The Bluetooth Profiles

The first one generic access profile is not really an application, but rather the basis upon which the real applications are built. Its main job is to provide a way to establish and maintain secure links between the master and slaves. Also relatively generic is the service discovery profile, which is used by devices to discover what services other devices have to offer. These two profiles are necessary for all Bluetooth devices. The remaining ones are optional.

The serial port profile is a transport protocol that most of the remaining profiles use. It emulates a serial live and useful for legacy applications. The generic object exchange profile defines a client-server relationship for moving data around. The next three profiles are for networking. The LAN access profile allows a Bluetooth device to connect to a fixed network. This profile is a direct competitor to 802.11. The dial-up network protocol is used to allow a notebook computer to connect to a mobile phone containing a built-in modem without wires.

The fax profile is similar to dial-up networking except that it allows wireless fax machines to send and receive faxes using mobile phones without a wire between the two.

The next three profiles cordless telephony, intercom, headset profiles are for telephony. The remaining three profiles are for actually exchanging objects between two wireless devices. These could be business cards, pictures, or

data files. The synchronization profile, in particular, is intended for loading data into a PDA or notebook computer when it leaves home and collecting data from it when it returns.

Q.56. Compare a piconet and scatternet. *(R.G.P.V., Dec. 20*

Ans. Compare a piconet and scatternet are as follows –

S.No.	*Piconet*	*Scatternet*
(i)	In this bluetooth network, device can function either as master or slave.	In this bluetooth network device can function as master or slave or (master + slave).
(ii)	It serves smaller coverage area.	It serves larger coverage area.
(iii)	It supports maximum 8 nodes.	It supports more than 8 nodes.
(iv)	It is allows less efficient use of available bluetooth channel band-width.	It allows more efficient use of available bluetooth channel band-width.

Also refer the ans. of Q.55.

NUMERICAL PROBLEMS

Prob.8. Evaluate the ring latency of 20 stations separated by 100 meters and operate at a speed of 4 Mbps. Assume the delay introduced by each station to be 2.5 bit. *(R.G.P.V., Dec. 20*

Sol. Given, Stations, M = 20, Speed, R = 4 Mbps and b = 2.5 bit.

The ring latency (in bits) is given as,

$$= \frac{20 \times 100 \times 4 \times 10^6}{2 \times 10^8} + 20\,(2.5) = 40 + 50 = 90 \text{ bits}$$ Ans.

UNIT 4

NETWORK LAYER

NETWORK LAYER – NEED, SERVICES PROVIDED, DESIGN ISSUES, ROUTING ALGORITHMS – LEAST COST ROUTING ALGORITHM, DIJKSTRA'S ALGORITHM, BELLMAN-FORD ALGORITHM, HIERARCHICAL ROUTING, BROADCAST ROUTING, MULTICAST ROUTING

Q.1. Discuss the need of network layer. What are the basic design issues of a network layer ?

Ans. The ***network layer*** is responsible for routing a packet within the subnet, i.e., from the source to the destination nodes across multiple nodes in the same network, or across multiple networks. This layer ensures the successful delivery of a packet to the destination node. To perform this, it has to choose a route. A route could be chosen before sending all the packets belonging to the same message (virtual circuit) or it could be chosen for each packet at each node (datagram). This layer is also responsible for tackling the congestion problem at a node, when there are too many packets stored at a node to be forwarded to the next node. Where there is only one small network based on broadcast philosophy (e.g., a single Ethernet LAN), this layer is either absent or has very minimal functionality.

The basic design issues of a network layer include the services provided to the transport layer, routing of packets through the subnet, congestion control, and connection of multiple networks together (internetworking).

Q.2. Datagram networks route each packet as a separate unit, independent of all others. Virtual circuit networks do not have to do this, since each data packet follows a predetermined route. Does this observation mean that virtual circuit networks do not need the capability to route isolated packets from an arbitrary source to an arbitrary destination ? Explain your answer. *(R.G.P.V., Dec. 2015)*

Ans. Virtual circuit most certainly requires this capability in order to route connection setup packet from an arbitrary source to an arbitrary destination.

Q.3. Describe a way to do reassembly of IP fragments at the destination. ***(R.G.P.V., Dec. 2***

Ans. For general case, the problem is nontrivial. Fragments may be out or order and some can be missing. On a retransmission, the datagram fragmented in different chunks size. In addition, the total size is not known until the last fragment receives. Probably the only way to manage reassembly is to buffer all the pieces until the last fragment receives and the size is known. Then build a buffer of the right size and put the fragments into the buffer maintaining a bit map with one bit per 8 bytes to keep track of which bytes are present in the buffer. The datagram is complete when all the bits are one in the bit map.

Q.4. Explain the services provided by the network layer to the transport layer.

Ans. Network layer provides services to the transport layer at the network layer/transport layer interface. Oftenly, this interface has a great importance due to another reason – it frequently is the interface between the carrier and the customer, that is, the boundary of the subnet. Carrier often consists of the control of the protocols and interface upto and including the network layer. Its function is to deliver packets given to it by its customers. Due to this reason this interface must be especially well defined. Network layer services have been designed with the following goals –

(i) Transport layer should be shielded from the number, type, and topology of the routers present.

(ii) Services should be independent of the router technology.

(iii) Network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

With these goals, designers of the network layer have a lot of freedom in writing detailed specifications of the services to be provided to the transport layer. This freedom degenerates into a raging battle between two warring factions. Center of the discussion is, whether the network layer should provide connectionless service or connection-oriented service.

According to one camp (represented by the Internet community), argues that the routers' job is moving packets around and nothing else. According to them, the subnet is inherently unreliable, no matter how it is designed. Therefore the hosts should accept the fact that network is unreliable and perform error control and flow control themselves. This thinking leads quickly to the conclusion that network service should be connectionless, with primitives SEND PACKET and RECEIVE PACKET and little else. Particularly, no packet ordering and flow control should be done, since the hosts are going to do that anyway, and there is usually little to be gained by doing it twice. In addition,

each packet must carry the full destination address, because each packet transmitted is carried independently of its predecessors, if any.

On the other hand, the argument of the other camp is that the subnet should provide a reliable, connection-oriented service. In this view, quality of service is the main factor and quality of service is not easy to obtain without connections in the subnet, especially for real-time traffic such as video and voice.

Best examples of these camps are Internet and ATM. Internet provides connectionless network layer service and ATM networks provide connection-oriented network layer service. But, it is interesting to notice that as quality of service guarantees are becoming more and more important, the Internet is evolving.

Q.5. What is routing ? ***(R.G.P.V., May/June 2006, Dec. 2015)***

Ans. Almost everyone is familiar with the general concept of routing. It means that if anyone wants to go from point A to point B, he has to decide a path to go there. In the same way, if anybody wants to transfer information between computers situated at two different locations which are connected via a WAN, network protocols must decide how to get it there.

In the case of LANs, organized around a single bus or ring, routing is not a problem. If their connection is with the bridges, the bridges make the routing decisions. Topologies are not very complex and bridges perform the routing rather easily.

Q.6. What do you mean by routing algorithms ?

Ans. The routing algorithms are a part of the network layer software. These algorithms are responsible for deciding the outgoing path for an incoming packet. In most subnets, packets will need multiple hops for travelling. Algorithms that select the routes and the data structures that they use are a major area of network layer design.

Routing algorithm is a process by which a routing table is defined. Routing table is the part of the network layer software which is responsible for deciding, which output line an incoming packet should be transmitted on.

Q.7. Write the desired properties of routing algorithm. ***(R.G.P.V., Dec. 2016)***

Ans. Desirable properties of routing algorithms are as follows –

(i) Correctness – It should get packets eventually to the correct destination.

(ii) Simplicity – This usually implies faster.

(iii) Stability – It should converge to some equilibrium under constant conditions.

(iv) Robustness – It should be able to handle new routers coming online, as well as, handle other going off or malfunctioning.

(v) Fairness and Optimality – These are hard to simultaneously satisfy. For example, in the situation below it might occur that to optimize flow would not allow traffic between X and X', a situation which is not fair.

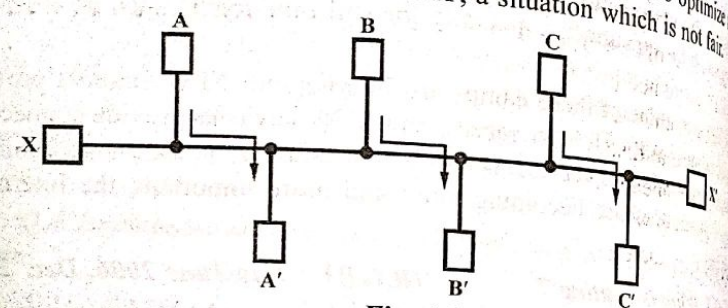


Fig. 4.1

Q.8. Differentiate between adaptive and non-adaptive routing algorithms. ***(R.G.P.V., May/June 2006, Dec. 2006, June 2013)***

Or

Define the types of routing algorithms. ***(R.G.P.V., June 2010)***

Ans. Routing algorithms are of two types – non-adaptive and adaptive. Non-adaptive algorithms are the algorithms that do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from i to j is calculated in advance, off-line, and downloaded to the IMPs when the network is booted. This procedure is also known as ***static routing.*** For example – shortest path routing, flooding and flowbased routing.

Adaptive algorithms are the algorithms that attempt to change their routing decisions to reflect changes in the topology and the current traffic. This is also called dynamic routing. For example – distance vector routing, link state routing, broadcast routing. There are three types of adaptive algorithms based on the information they use. The global algorithms use information collected from the entire subnet in an attempt to make optimal decisions. This approach is called centralized routing. The local algorithms run separately on each JMP and only use information available there, such as queue lengths. These are known as isolated algorithms. Lastly, there is a third class of algorithms that uses a mixture of global and local information. They are called distributed algorithms.

Q.9. What do you mean by routing ? What are various types of routing algorithms ? Explain any one. ***(R.G.P.V., June 2011)***

Ans. **Routing** – Refer the ans. of Q.5.

Types of Routing Algorithms – Refer the ans. of Q.8.

Q.10. Discuss least cost routing algorithm. ***(R.G.P.V., Dec. 2006)***

Ans. The decision of the least-cost routing depends on efficiency – which of the available pathways is the cheapest or, in networking terminology, the shortest. A value is assigned for each link; the length of a particular route is equal to the total value of the component links. In this context, the term shortest can mean either of two things depending on the protocol. In few cases, shortest means the route needing the smallest number of relays or hops. For example, a direct link from A to D would be considered shorter than the route A–B–C–D even if the actual distance covered by the latter is the same or less. For other cases, shortest means fastest, cheapest, most reliable, most secure or best of any other quality which can make one particular link (or combination of links) more attractive than another. Generally, shortest means a combination of all of these.

In hop-count routing, shortest means the pathway needing the smallest number of relays, in which every link is considered to be of equal length and given the value one. Hop-count routing becomes by using equal link values. One-hop routes are always equal to one, two-hop routes are always equal to two and so on. Routes require updating only when a link becomes unavailable. In that case, the value of the link becomes infinite and an alternate is obtained. Usually, hop-count algorithms control the routes known by a single user to those within 15 hops. A particular hop-count algorithm may be customized for transmissions with special needs (e.g., military transmissions which need highly secure lines). In these cases, few links will be given a value of one, while others will have higher values and will be avoided.

Other protocols factor a number of qualities related to the functioning of a link before assigning a value to a link. Speed, traffic congestion and link medium (telephone line, satellite transmission, etc.) are these qualities. If all relevant factors for a particular link are combined, a number which represents the value or length of the link is issued. This number shows an assessment of efficiency, not a physical distance, it is known as the symbolic length of the link.

Based on whatever qualities are considered important to that network, each link in a network is assigned a link in some protocols. When the link between two routers is half-duplex or full-duplex (has two way traffic), the length of the link in one direction might be different from the length of the link in other direction. Other factors, such as traffic load or quality of the cable, may differ except the physical distance which the signal has to travel. As with hop-count routing, the decision of which route is best, is based on the shortest distance, calculated by totaling the lengths of every link used by a given path. In the case of hop-count routing, all three-hop paths have a total length of three and are considered longer than two-hop paths. However, the total length

of a three-hop link may turnout to be shorter than that of a two-hop link, when different links are assigned different lengths.

Q.11. How does link state routing take care of the problem of wrapping of sequence numbers, crashing of routers and corruption of sequence number? ***(R.G.P.V., June 2009)***

Ans. The link state routing has a some problem as –

(i) Here, confusion will reign because of the sequence numbers wrap around. This can be reduced by using a 32-bit sequence number. It would consider 137 years to wrap around with one link state packet per second, therefore this possibility can be eliminated.

(ii) It will lose track of its sequence number when a router ever crashes. The next packet will be rejected as a duplicate when it starts again at zero.

(iii) Because the current sequence number is thought to be 65540 if a sequence number is ever damaged and 65540 is received instead of 4 (a one bit error), packet 5 through 65540 will be rejected as obsolete.

These problem can be solved by the age of every packet after the sequence number and decrement it one per second. The information from that router is removed when the age hits zero. Generally, a new packet comes in every 10 sec., therefore router information only times out if a router is down. During the initial flooding process, the age field is also decremented by each router, to make sure no packet can obtain lost and live for an indefinite time period.

Q.12. What are unicast routing protocols ? ***(R.G.P.V., June 2010)***

Ans. Unicast routing protocol is a combination of governing rules and procedures that help routers to inform each other in case of any changes. It also permits routers to share whatever they know about the Internet or their neighbourhood. Unicast routing protocols may also be classified as intradomain and interdomain routing protocols.

Thus, routing between autonomous system is known as interdomain routing and routing inside an autonomous system is known as intradomain routing.

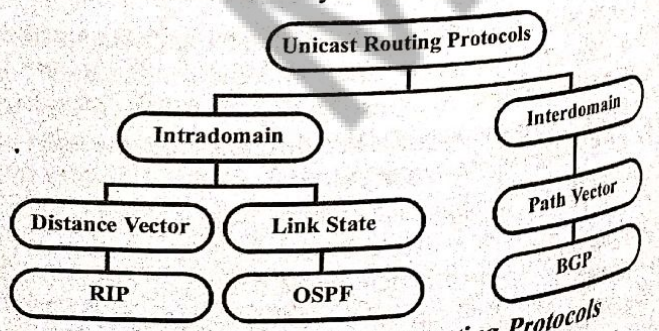


Fig. 4.2 Popular Unicast Routing Protocols

(i) RIP (Routing Information Protocol) – RIP is an intradomain routing protocol. It is based on distance vector routing. It implements distance vector routing directly with some considerations –

(a) We deal with routers and networks (links) in an autonomous system. Network does not have any routing table. In contrast, routers have it.

(b) The destination in a routing table is a network. It means that the first column specifies a network address.

(c) RIP uses the metric. The distance can be defined as the number of networks (links). That is why, the metric in RIP is known as a hop count.

(d) RIP defines infinity as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.

(e) The next-node column specifies the address of the router to which the packet is to be sent to reach its destination.

(ii) OSPF Protocol – It is an intradomain routing protocol and based on link state routing. OSPF protocol can be understood by defining it in area.

An area is a collection of networks, hosts, and routers all contained within an autonomous systems. Although, we can divide an autonomous system in many working areas. All networks inside an area should be connected. Routing information is flooded by routers in areas. Special routers called area border routers are attached at the border of an area to summarize the information about area and send it to other areas. A backbone area is a special area and all other areas inside an autonomous system must be connected to the backbone. This backbone area is called primary area and other areas are considered as secondary areas. Each area has an area identification. The area identification of the backbone is zero.

(iii) BGP – Border gateway protocol (BGP) is an interdomain routing protocol using path vector routing. In BGP, any exchange of routing information between two routers takes place in a session. A session can be defined as a connection between two BGP routers only for exchanging the routing information. BGP also uses the services of TCP for creating a reliable environment. As an application program, a session at BGP level is a connection at the TCP level. When a TCP connection is established for BGP, it can last for a long time, until something unusual happens. That's why, BGP sessions are sometimes known as semi permanent connections.

BGP can have two kinds of sessions – external BGP (E-BGP) and internal BGP (I-BGP) sessions. Both of these sessions are different from each other in their functionality. The E-BGP session is used to exchange information between two nodes belonging to two different autonomous systems. In contrast, I-BGP session is used to exchange routing information between two routers inside an autonomous system. We can understand these sessions by fig. 4.3.

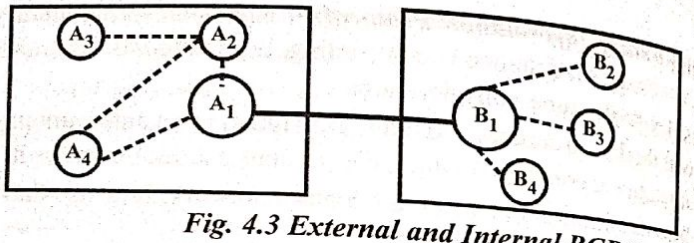


Fig. 4.3 External and Internal BGP Sessions

Q.13. Give the algorithm to find the shortest path in the following weighted graph. Also find the shortest path.

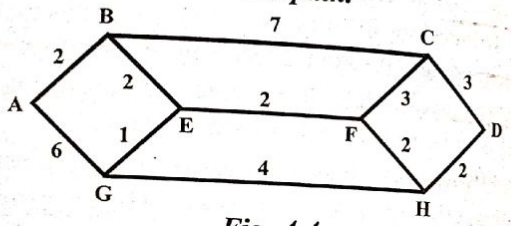


Fig. 4.4

(R.G.P.V., Dec. 2003, May/June 2006, Nov./Dec. 200

Or

Explain Dijkstra's algorithm with example.

(R.G.P.V., June 2009, Dec. 200

Ans. This technique is widely used in many forms because it is simp and easy to understand. The idea is to make a graph of the subnet, with eac node of the graph representing a router and each arc of the graph represent a communication line (often known as a link). For selecting a route betwee given pair of routers, the algorithm just finds the shortest path between the on the graph.

One method of measuring path length is the number of hops. Using t metric, the paths ABC and ABE are equally long as shown in fig. 4.5. Anoth metric is the geographic distance in kilometres, in which case ABC is muc longer than ABE.

Several other metrics are also possible besides hops and physical distanc As an example, each arc could be labeled with the mean queueing an transmission delay for some standard test packet as determined by hourly te runs. The shortest path is the fastest path with this graph labeling, rather tha the path with the fewest arcs or kilometres.

Generally, the labels on the arcs could be computed as a function of t distance, bandwidth, average traffic, communication cost, mean queue lengt measured delay and other factors. Then the algorithm would compute th "shortest" path by changing the weighting function, measured according t any one of a number of criteria or a combination of criteria.

Many algorithms for computing the shortest path between two nodes of a graph are known. Every node is labeled with its distance from the source node along the best known path. In starting, paths are not known, therefore all nodes are labeled with infinity. As the algorithm proceeds and paths are obtained, the labels may change, reflecting better paths. A label may be either permanent or tentative. All labels are tentative in starting. When it is discovered that a label shows the shortest possible path from the source to that node, it is made permanent and never changed thereafter.

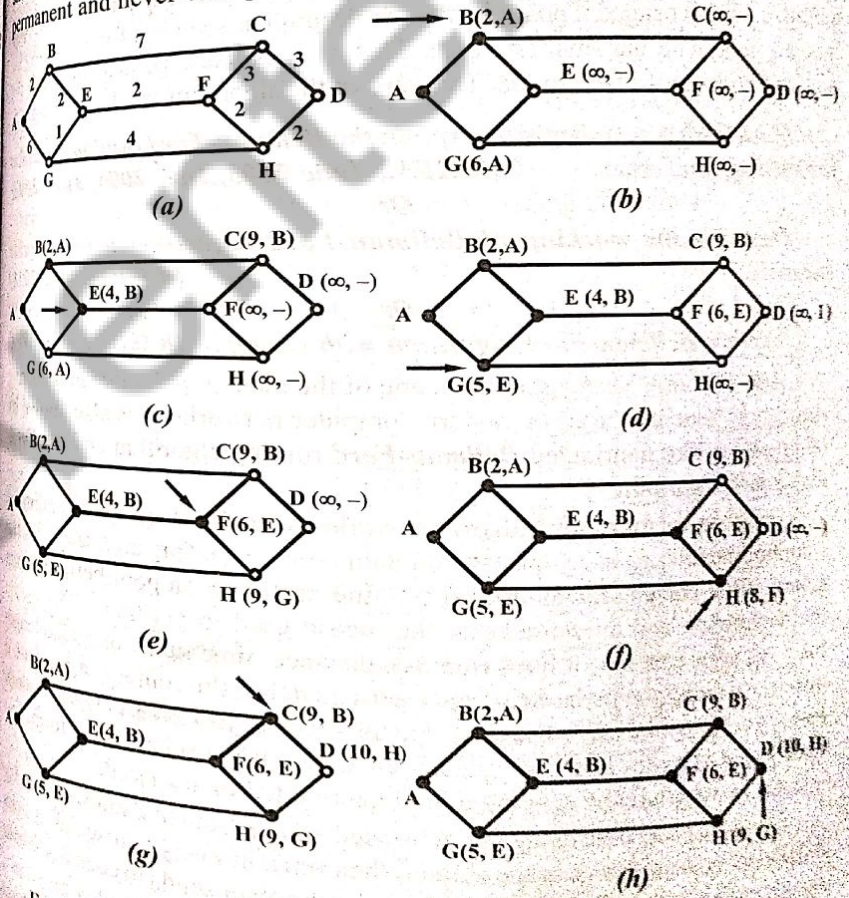


Fig. 4.5

For illustrating the working of labeling algorithm see at the weighted, undirected graph of fig. 4.5 (a) in which the weights represent distance. For finding the shortest path from A to D. We start out by marking node A as permanent, denoted by a filled-in circle. Then, each of the nodes adjacent to A (the working node), relabeling each one with the distance to A. Whenever a node is relabeled, it is also labeled with the node from which the probe was

made, therefore the final path can be constructed later. After examining ea
of the nodes adjacent to A, all the tentatively labeled nodes are examined to
whole graph and made the one with the smallest label permanent as shown
fig. 4.5 (b). This one is the new working node.

Now, starting is done from B and all nodes adjacent to it are examined. If
sum of the label on B and the distance from B to the node being considered is les
than the label on that node, a shorter path is obtained, therefore the label is relabeled

When all the nodes adjacent to the working node have been inspected and th
tentative labels changed if possible, the whole graph is searched for the tentativ
labeled node with the smallest value. This node is made permanent and is ma
working node for the next round. The steps of the algorithm are shown in fig 4.

Q.14. With a neat diagram, explain the Bellman-Ford routing algorithm for routing packets. ***(R.G.P.V., June 2003, Dec. 2005, June 200***

Or

Describe the working of Bellman-Ford algorithm using suitable example. ***(R.G.P.V., May 20***

Or

Explain Bellman-Ford algorithm with example. ***(R.G.P.V., May 20***

Ans. Distance vector routing is one of the most popular dynamic routing algorithms generally used in modern computer networks. It is also known by other names like distributed ***Bellman-Ford*** routing algorithm and the ***Ford-Fulkerson*** algorithm.

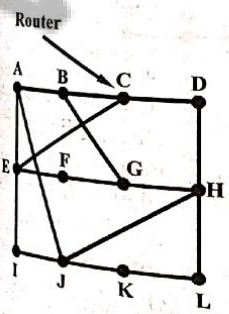
Distance vector routing algorithm works by having each router maintain a routing table (i.e., a vector) that contains one entry for, each router in the subnet. This entry contains two parts – the preferred outgoing line to reach the destination and an estimate of the metric used to get there. The metric used might be number of hops (jumps), distance, time delay or queue-length of packets along the path, etc. If the metric is delay, the router can measure directly with special ECHO packets that the receiver just timestamps and sends back as fast as it can. The routing tables are updated by exchanging information with the neighbours, by sending a list of estimated metric used.

Suppose if the time delay metric is used and the router Y knows the delay to each of its neighbours in the subnet, then once in every T msec all routers exchange the information with each other. Each router sends to each neighbour a list of its estimated delays to each destination. It (router Y) also receives a similar list from each neighbour. Imagine that it receives a list from its neighbour router X, showing its estimate of X_i, the time it takes to reach the router i. Now the router Y knows that the delay (time taken) to X is m msec, so it can reach to router i via X in X_i + m msec. Using this calculation, routers can find the best estimate and use that estimate and the corresponding line in its new routing table.

Let us consider an example with the help of the following fig. 4.6.

We are given a subnet as shown in fig. 4.6 (a). The aim is to find the best route from router J to router G. The metric used is time delay. The first four columns of fig. 4.6 (b) show the delay vectors received from the neighbours of router J. In the first column, A claims to have a 12 msec delay to reach to B, a 25 msec delay to C, a 40 msec delay to D, etc. Suppose J has already estimated its delay to reach its neighbours, A, I, H and K as 8, 10, 12 and 6 msec, respectively.

Now since J can get to A in 8 msec and A claims to be able to get to G in 18 msec, so the total delay from J to get to G, via A is (8 + 18) msec, i.e., 26 msec. Similarly, it computes the total delay to G, via other neighbours. Like, via I is (10 + 31) = 41 msec, via H is (12 + 6) = 18 msec and via K is (6 + 31) = 37 msec. The best of these values is 18 msec (shortest delay). Thus, J finds the best route to get to G via H. The same calculation can be performed for all other destinations thus updating to give new routing table for J.



(a) A Subnet

To	A	I	H	K	New Estimated Delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA Delay is 8	JI Delay is 10	JH Delay is 12	JK Delay is 6		New Routing Table for J

Vectors Received From J's Four Neighbors

(b) Inputs From A, I, H, K and the New Routing Table for J

Fig. 4.6

Applications of Distance Vector Routing – This algorithm is used in ARPANET, Internet, early versions of DEC net and Novell's IPX, Apple Talk and Cisco routers.

There are two primary drawbacks in distance vector routing –

(i) First, for choosing the routes, it considers queue length as delay metric and does not take line bandwidth into account.

(ii) Second, the algorithm converges very slowly, even with tricks like split horizon.

Q.15. Write short note on count to infinity problem.

Or

How count-to-infinity problem is generated in routing algorithm ? ***(R.G.P.V., June 20***

(R.G.P.V., Dec. 20

Ans. Bellman-Ford routing or distance vector routing works in theory but has a serious drawback in practice – although it converges to the correct answer, it may do so slowly. In particular, it reacts rapidly to good news, but leisurely to bad news. Assume a router whose best route to destination X is large. If on the next exchange neighbour A suddenly reports a short delay to X, the router just switches over to using the line to A to send traffic to X. In one vector exchange, the good news is processed.

To see how fast good news propagates, consider the five-node (linear) subnet of fig. 4.7, in which the delay metric is the number of hops. Let A be down initially and all the other routers know this. In other words, they have recorded the delay to A as infinity.

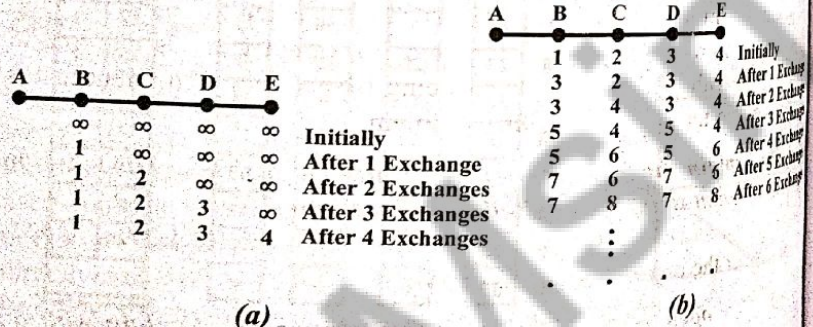

A B C D E
∞ ∞ ∞ ∞ Initially
1 ∞ ∞ ∞ After 1 Exchange
1 2 ∞ ∞ After 2 Exchanges
1 2 3 ∞ After 3 Exchanges
1 2 3 4 After 4 Exchanges
(a)
A B C D E
1 2 3 4 Initially
3 2 3 4 After 1 Exchange
3 4 3 4 After 2 Exchange
5 4 5 4 After 3 Exchange
5 6 5 6 After 4 Exchange
7 6 7 6 After 5 Exchange
7 8 7 8 After 6 Exchange
(b)

Fig. 4.7 The Count-to-infinity Problem

If A comes up, the other routers learn about it via the vector exchanges. For simplicity, we will assume that there is a gigantic gong somewhere that is struck periodically to initiate a vector exchange at all routers simultaneously. At the time of the first exchange, B learns that its left neighbour has zero delay to A at the time of the first exchange. Now B makes an entry in its routing table that A is one hop away to the left. All the other routers still think that A is down. At this point, the routing table entries for A are as illustrated in the second row of fig. 4.7 (a). On the next exchange, C learns that B has a path of length 1 to A, so it updates its routing table to represent a path of length 2, but D and E do not hear the good news until later. Clearly, the good news is spreading at the rate of one hop per exchange. In a subnet whose longest path is of length N hops, within N exchanges everyone will know about newly revived lines and routers.

Now assume the situation of fig. 4.7 (b), where all the lines and routers are initially up. Routers B, C, D and E have distances to A of 1, 2, 3 and 4 respectively. Suddenly A goes down, or alternatively the line between A and B is cut, that is effectively the same thing from B's perspective.

B does not hear anything from A at the first packet exchange. Fortunately, C says "Do not worry. I have a path to A of length 2." Little does B know that C's path runs through B itself. For all B knows, C might have ten outgoing lines all with independent path to A of length 2. As a result, B now thinks it can reach A via C, with a path length of 3. D and E do not update their entries for A on the first exchange.

On the second exchange, C notices that each of its neighbours claims to have a path to A of length 3. It picks up one of them at random and makes its new distance to A 4, as illustrated in third row of fig. 4.7 (b). Subsequent exchanges create the history shown in the rest of fig. 4.7 (b).

Thus, it is clear from this figure that why bad news travels slowly – no router has a value more than one higher than the minimum of all its neighbours. Gradually, all routers work their way upto infinity, but the number of exchanges required depends on the numerical value used for infinity. Due to this reason, it is wise to set infinity to the longest path plus 1. When the metric is time delay, there is no well-defined upper bound, so a high value is required to prevent a path with a long delay from being treated as down. Hence, this problem is called the ***count-to-infinity*** problem.

Q.16. Explain the Bellman-Ford routing algorithm. Discuss the drawback of count to infinity in Bellman-Ford algorithm.

(R.G.P.V., Dec. 2017)

Ans. Refer the ans. of Q.14 and Q.15.

Q.17. How open shortest path first (OSPF) work ? Explain with an example.

(R.G.P.V., June 2016)

Ans. OSPF supports point-to-point and multiaccess networks. It operates by abstracting the collection of actual networks, routers and lines into a directed graph in which each arc is assigned a cost. Then, it determines the shortest path on the basis of weights on the arcs. A pair of arcs one in each direction represents a serial connection between two routers. Their weights may be different. OSPF is a link state protocol. In a link state protocol, a router does not exchange distances with its neighbours. Instead each router actively tests the status of its link to each of its neighbour, which then propagate it throughout the autonomous system. Each router takes this link state information and builds a complete routing table.

Many of the autonomous systems in the Internet are themselves l and nontrivial to manage. OSFP breaks them into numbered areas. An area a network or a set of contiguous networks. Areas do not overlap but need be exhaustive, that is, some routers may not belong to an area. An area generalization of a subnet and its topology and details are invisible outside area. Every autonomous system contains backbone area known as area 0. areas are connected to the backbone by tunnels. In the graph, a tunnel represented by an arc and contain a cost. Each router that is connected to or more areas is part of backbone. Each router has the same link state databa and runs the same shortest path algorithm within an area. A router that connect to two areas needs the database for both areas and must run the shortest p algorithm for each one separately. In OSPF following types of routes required – intra-area, inter-area and inter-AS. As the source router knows shortest path to the destination router, intra-area routes are the easiest. Th are three steps in inter-area routes – go from the source to the backbone across the backbone to the destination area and go to the destination.

OSPF works by exchanging information between adjacent routers, wh is not the same as between neighbouring routers. It is inefficient to have ev router on a LAN talk to every other router on the LAN. Thus, one rout elected as the designated router. It is said to be adjacent to all the other rout on its and exchanges information with them. Neighbouring routers that are adjacent do not exchange information with each other. A backup desig router is always kept up-to-date. Each router periodically floods LINK STA UPDATE messages to each of its adjacent routers during normal operation. T message gives its state and gives the costs used in the topological database. T flooding messages are acknowledged to make them reliable. These messages also sent by the routers when a line goes up or down or its cost chan DATABASE DESCRIPTION message give the sequence numbers of all the state entries currently held by the sender. These messages are used when is brought up. Either partner can request link state information from the o one by using LINK STATE REQUEST messages. The result of this algorithm that each pair of adjacent routers checks to see who has the most recent and new information is spread throughout the area this way. All these messa are sent as raw IP packets. Finally, we can put all the pieces together. U flooding, each router informs all the other routers in its area of its neighb and costs. This information allows each router to construct the graph for areas and compute the shortest path. The backbone area does this too.

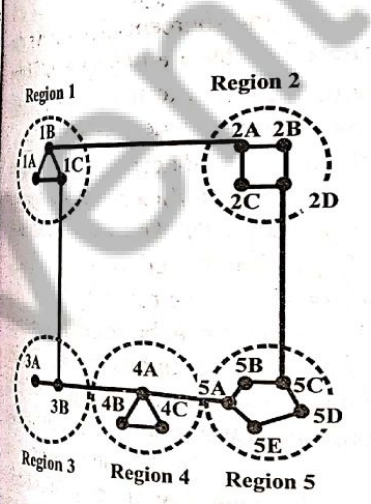
Q.18. Write short note on hierarchical routing.

Ans. Sometimes there are too many nodes to provide each one with a information efficiently. Treating each node as an equal participant in a network generates too much information to share and transmit through

network. An alternative is to have some nodes do the routing for others. A common approach is hierarchical routing.

In hierarchical routing, the routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions. If different networks are connected together, then it is natural to regard each one as a separate region in order to free the routers in one network from having to know the topological structure of the other ones.

In large networks, a two-level hierarchy may be insufficient. It may be essential to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.



(a)

Full Table for 1A

Dest.	Line	Hops
1A	—	—
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical Table for 1A

Dest.	Line	Hops
1A	—	—
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Fig. 4.8 Hierarchical Routing

A quantitative example of routing in a two-level hierarchy with five regions is given in fig. 4.8 (a). As shown in fig. 4.8 (b), the full routing table for router 1A has 17 entries. If routing is performed hierarchically as in fig. 4.8 (c), there are entries for all the local routers as before, but all other regions have been condensed into a single router. Therefore, all traffic for region 2 goes via the 1B–2A line, but the remaining of the remote traffic goes via the 1C–3B line. Hierarchical routing has reduced the table from 17 to 7 entries. When the ratio of the number of regions to the number of routers per region grows, the savings in table space increase.

But, these gains in space are not free. There is a penalty to be paid. This penalty is in the form of increased path length. As an example, the best route from 1A to 5C is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.

In the case if a single network becomes very large, Kamoun and Kleinrock have discovered that the optimal number of levels for an N router subnet is ln N, requiring a total of e ln N entries per router. They have also indicating the the increase in effective mean path length caused by hierarchical routing is sufficiently small which is usually acceptable.

As an example, assume a subnet with 720 routers. Each router requires 720 routing table entries when there is no hierarchy. When the subnet is divided into 24 regions of 30 routers each, every router requires 30 local entries plus 23 remote entries for a total of 53 entries. When a three-level hierarchy is selected with eight clusters, each having 9 regions of 10 routers, each router requires 10 entries for local routers, 8 entries for routing to other regions within its own cluster, and 7 entries for distant clusters, for a total of 25 entries.

Q.19. Discuss broadcast and multicast routing algorithm.
(R.G.P.V., Dec. 2009, June 2010

Ans. (i) Broadcast Routing – There are some applications, in which hosts require to transmit messages to many or all other hosts. For example, a service distributing weather reports, stock market updates, or live radio programs might work best by broadcasting to all machines and letting those which are interested read the data. Transmitting a packet to all destinations simultaneously is known as ***broadcasting.***

Various techniques have been proposed for it –

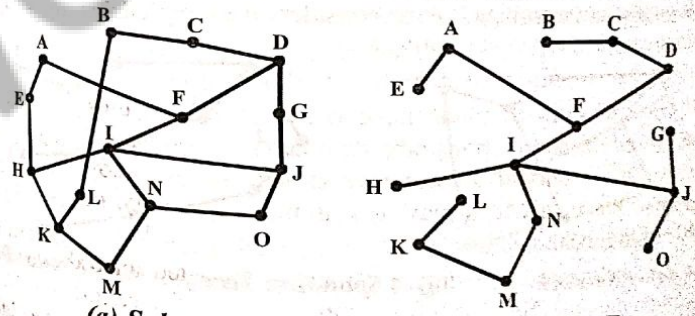
First broadcasting technique that needs no special features from the subnet is for the source to simply transmit a distinct packet to each destination. This technique wastes bandwidth and needs source to have a complete list of all destinations. Practically, this may be the only possibility, but it is the least desirable of the techniques.

Second technique is flooding. Flooding is ill-suited for ordinary point-to-point communication. But, for broadcasting it might rate serious consideration especially when none of the techniques described below are applicable. Problem with flooding as a broadcast method is the same problem it has as a point-to-point routing algorithm. It produces too many packets and takes too much bandwidth.

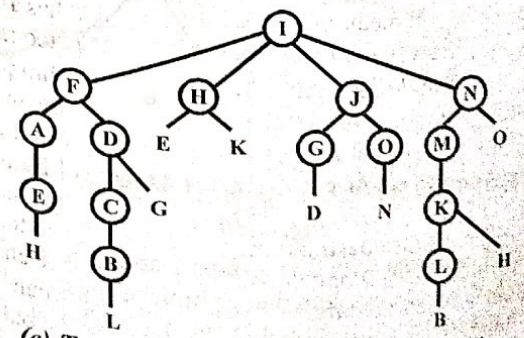
Third algorithm is multidestination routing. This technique is used when each packet contains either a list of destinations or a bit map showing the desired destinations. If a packet arrives at a router, then router checks all the destinations to obtain the set of output lines which will be required. Router produces a new copy of the packet for each output line to be used and includes in each packet only for those destinations which are to use the line. In effect, the destination set is divided among the output lines. After a enough number of hops, each packet will carry only one destination and can be treated as a normal packet. Multidestination routing is similar to the separately addressed packets, except that if many packets must follow the same route, one of them pays full fare and the rest ride free.

In fourth technique, sink tree is explicitly used for the router initiating the broadcast, or any other convenient spanning tree is used for that matter. A spanning tree is a subset of the subset which includes all the routers but contains no loops. When each router knows which of its lines belong to the spanning tree, it can copy an incoming broadcast packet onto all the spanning tree lines except the one it arrived on. In this technique, bandwidth is used excellently and absolute minimum number of packets are generated which are essential to do the job. But, there is also a problem that each router must have knowledge of spanning tree for it to be applicable. Sometimes this information is available (for example, with link state routing) and sometimes it is not available (as an example, with distance vector routing).

The last broadcast algorithm is an effort to approximate the behaviour of the previous one, even if the routers do not know anything at all about spanning trees. The idea, called reverse path forwarding, is remarkably simple once it has been pointed out. If a broadcast packet arrives at a router, then router checks to see if the packet arrived on the line that is generally used for transmitting packets to the source of the broadcast. Therefore, when there is an excellent opportunity that the broadcast packet itself followed the best route from the router and is therefore the first copy to arrive at the router.



(a) Subnet *(b) Spanning Tree*



(c) Tree Built by Reverse Path Forwarding

Fig. 4.9 Reverse Path Forwarding

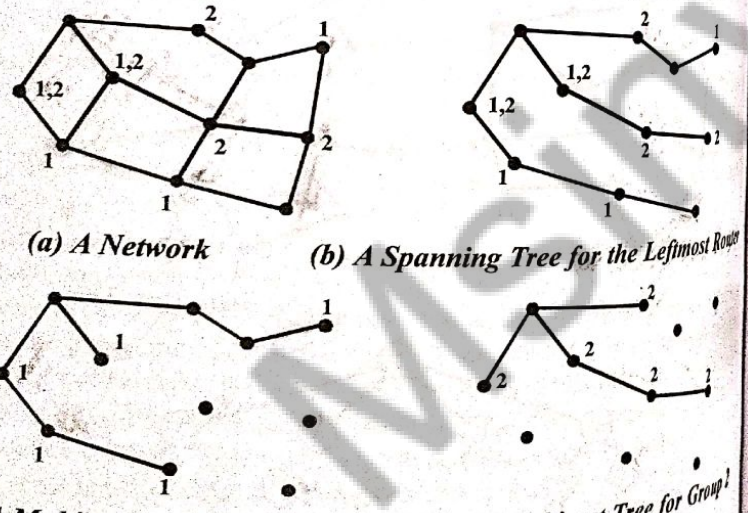
This being the case, router forwards copies of it onto all lines except one it arrived on. But, when the broadcast packet arrived on a line other than the preferred one for reaching the source, packet is discarded as a likely duplicate.

Fig. 4.9 shows an example of reverse path forwarding. Fig. 4.9 (a) shows a subnet, fig. 4.9 (b) shows a sink tree for router I of that subnet, and fig. 4.9 (c) shows how the reverse path algorithm works.

(ii) Multicast Routing – The procedure of sending a message to the group of widely separated processes in a network is called multicasting. The messages are sent to well-defined groups that are numerically large in size but small as compared to the network, as a whole. An example where different processes work together in groups is distributed database system. The routing algorithm is called ***multicast routing***.

Multicasting needs group management to generate and destroy groups and to permit processes to leave and join the groups. Multicast routing is concerned with the fact that when a process joins a group, it must inform its host. It is important that routers must know about which of their hosts belong to which group. As the routers tell their neighbours, the information propagates through the subnet.

In multicast routing, each router computes a spanning tree for itself, covering all other routers in the subnet. Let us consider an example given in fig. 4.10.



(a) A Network *(b) A Spanning Tree for the Leftmost Router*

(c) A Multicast Tree for Group 1 *(d) A Multicast Tree for Group 2*

Fig. 4.10

In fig. 4.10 (a), a subnet with two groups 1 and 2, is given. Some routers are connected to hosts that belong to one or both of these groups. A spanning tree for the left most router is illustrated in fig. 4.10 (b). If a process transmits a multicast packet to a group, the first router of the subnet forms a pruned spanning tree, removing all lines not leading to the hosts of the groups. In fig. 4.10 (c) and fig. 4.10 (d) pruned spanning trees for group 1 and group 2 are shown. Multicast packets are forwarded only along the suitable spanning tree. There are various algorithms used to prune the spanning tree; like link state routing, distance vector routing, reverse path forwarding, etc.

Q.20. Explain multicasting routing in brief. ***(R.G.P.V., June 2017)***

Ans. Refer the ans. of Q.19 (ii).

Q.21. What do you mean by routing ? Explain hierarchical, broadcast and multicast routing. ***(R.G.P.V., May 2019)***

Ans. Refer the ans. of Q.5, Q.18 and Q.19.

Q.22. What do you mean by unicast routing ? ***(R.G.P.V., Dec. 2016)***

Ans. Unicast communication has one source and one destination, i.e. the relationship between the source and the destination is one-to-one. In this type of communication, both the source and destination addresses, in the IP datagram, are the unicast addresses assigned to the hosts.

In unicast routing, when a router receivers a packet to forward, it needs to find the shortest path to the destination of the packet. The router consults its routing table for that particular destination. The next-hop entry corresponding to the destination is the start of the shortest path. The router knows the shortest path for each destination, which means that the router has a shortest path tree to optimally reach all destinations. In other words, each line of the routing table is a shortest path, the whole routing table is a shortest path free. In unicast routing, each router needs only one shortest path tree to forward a packet; however, each router has its own shortest path tree. The router may discard the packet if it cannot find the destination address in its routing table.

A ***unicast*** packet starts from the source S_1 and passes through routers to reach the destination D_1 as shown in fig. 4.11.

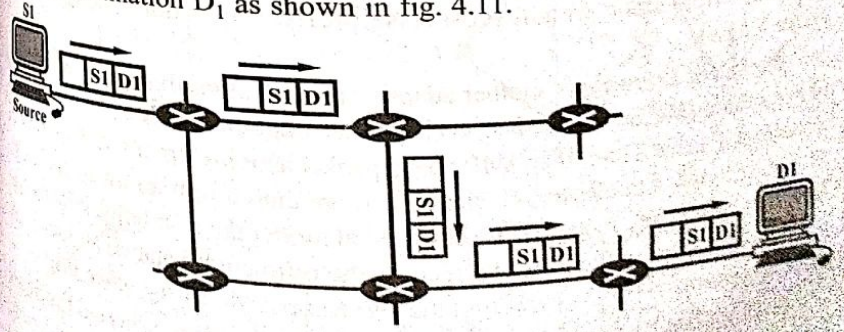


Fig. 4.11

Q.23. With the help of suitable diagrams explain unicast, multicast and broadcast routing. ***(R.G.P.V., June 2014)***

Ans. Refer the ans. of Q.22 and Q.19.

Q.24. What is the difference between unicast routing and multicast routing ? *(R.G.P.V., Dec. 2015)*

Ans. Refer the ans. of Q.22 and Q.19.

Q.25. What is the isolated routing ? Explain one isolated routing algorithm in details. *(R.G.P.V., Dec. 2016)*

Ans. Isolated adaptive routing is the simplest decentralized routing algorithm. The JMP make routing decisions based only upon information they themselves have gleaned, they do not exchange routing transmission per sec with other IMP. They also never try to adapt to changes in topology and traffic.

One simple isolated adaptive algorithm is Baran's ***Hot Potato*** algorithm. When a packet comes in, the IMP tries to get rid of it as fast as it can, by putting it on the shortest output queue. It means that when a packet arrives, the IMP counts the number of packets queued up for transmission on each of the output lines. It then attaches the new packet to the end of the shortest output queue without regard to where that line leads. In the fig. 4.12, the inside of IMP is shown at a certain instant of time. Here, the four output queues corresponds to the four output lines. Packets are queued up on each line waiting for transmission. Here in this example, queue I is the shortest, with only one packet queued up. Therefore, the Hot Potato algorithm put the newly arrived packet on this queue.

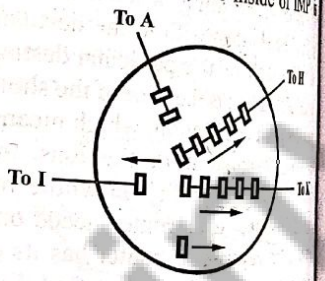


Fig. 4.12 Queuing within the IMP

A variation of this idea is to combine static routing with Hot Potato algorithm. Here static weight (cost wise preference is done along with the queue length).

Backward Learning is another adaptive routing algorithm. Here the identity of the source IMP is included in each packet, together with a counter that is incremented on each hop. If an IMP sees a packet arriving on line K from IMP H with hop count 4, it knows that H cannot be more than four hops away via line K. Now if its current best route to H is estimated at more than four hops, it marks line K as the choice for traffic to H and records the estimated distance as four hops. After some time, every IMP will find the shortest path to every other IMP.

Another similar routing technique is the ***delta routing*** where a threshold value δ is decided for cost difference between any path and its shortest path. All paths having δ less than or equal to δ are considered able for packet forwarding. When $\delta \to 0$ only shortest path is chosen and if $\delta \to \infty$ then all path are equally likely.

NUMERICAL PROBLEMS

Prob.1. What is Dijkstra algorithm ? Using Dijkstra algorithm find the shortest path from 0 to 4.

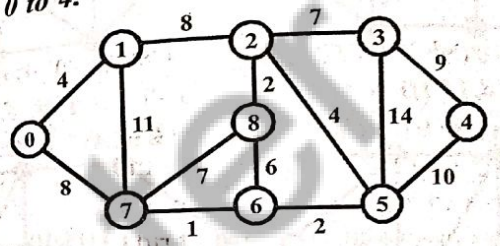


Fig. 4.13 *(R.G.P.V., June 2015)*

Sol. **Dijkstra Algorithm** – Refer the ans. of Q.13.

For simplicity, we can redrawn fig. 4.13 as fig. 4.14. The step by step execution of the Dijkstra's algorithm is shown in fig. 4.15 (a) to 4.15 (i).

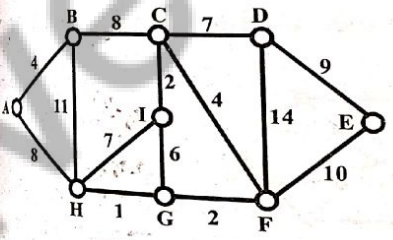


Fig. 4.14

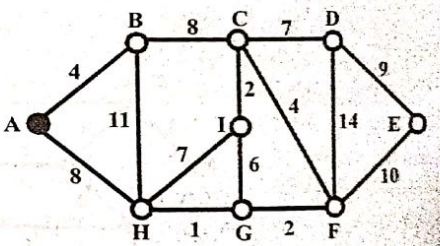


Fig. 4.15 (a)

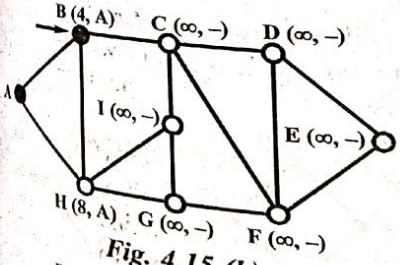


Fig. 4.15 (b)

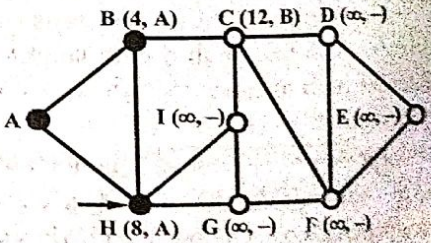


Fig. 4.15 (c)

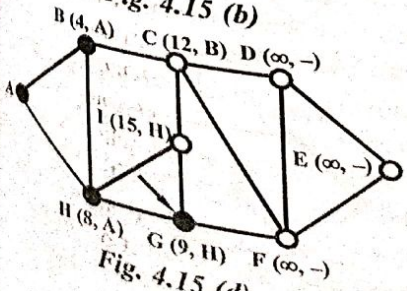


Fig. 4.15 (d)

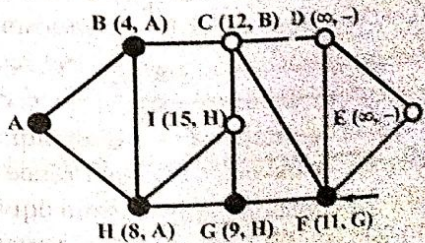


Fig. 4.15 (e)

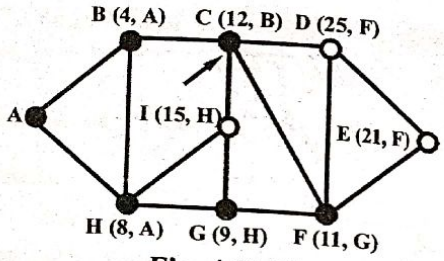


Fig. 4.15 (f)

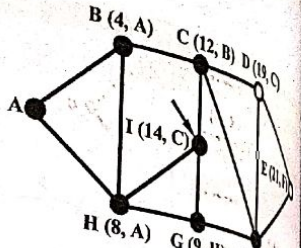


Fig. 4.15 (g)

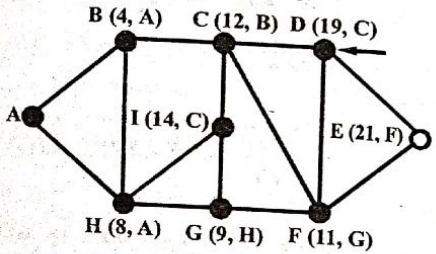


Fig. 4.15 (h)

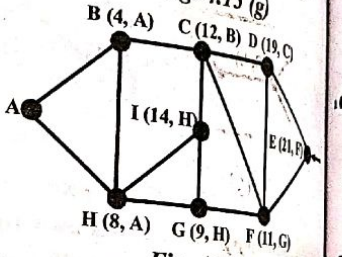


Fig. 4.15 (i)

Prob.2. Apply Dijkstra's routing algorithm to calculate shortest path with source vertex 'a'.

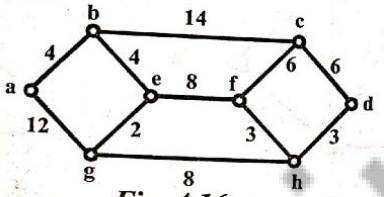
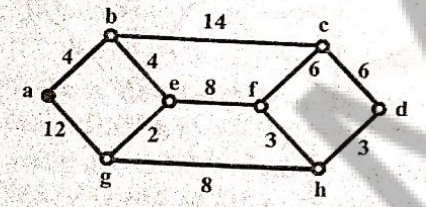
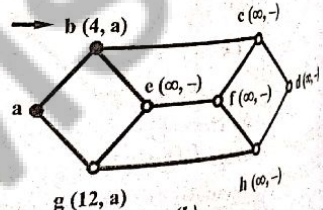


Fig. 4.16 *(R.G.P.V., Dec. 2018)*

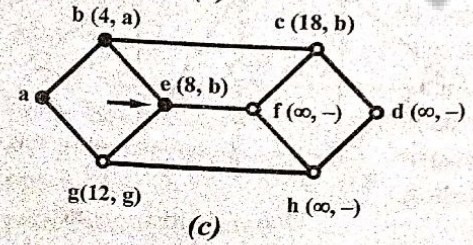
Sol. Fig. 4.17 shows the steps of Dijkstra routing algorithm to calculate shortest path from a to d with source vertex 'a'. It is clear from fig. 4.17 the shortest path abeghd.



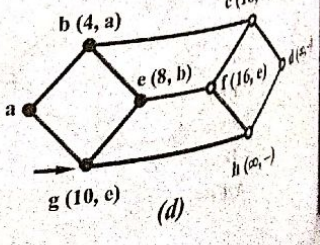
(a)



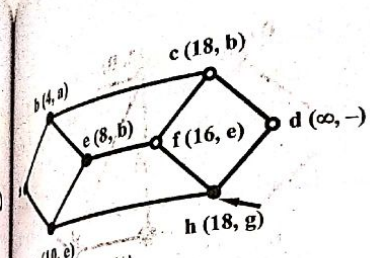
(b)



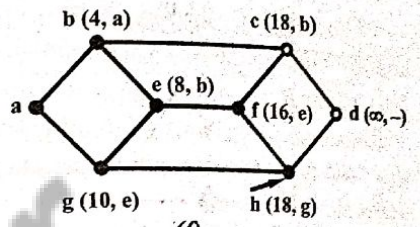
(c)



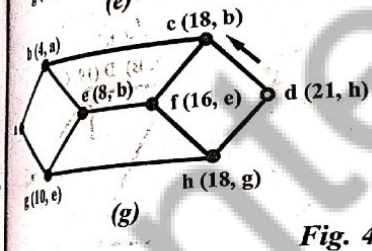
(d)



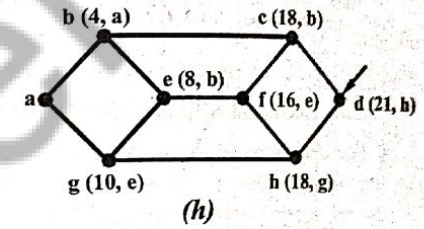
(e)



(f)



(g)



(h)

Fig. 4.17

IP ADDRESSES, HEADER FORMAT, PACKET FORWARDING, FRAGMENTATION AND REASSEMBLY, ICMP, COMPARATIVE STUDY OF IPv4 & IPv6

Q.26. What is logical address ?

Ans. A logical address in Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address. We use the term IP address to mean a logical address in the network layer of the TCP/IP protocol suite. The Internet addresses are 32 bits in length, this gives us a maximum of 2^{32} addresses. These addresses are referred to as IPv4 addresses or simply IP addresses.

Q.27. What is IP addresses ? Categorize the IP addresses into various classes. ***(R.G.P.V., June 2015)***

Ans. For addresses, the designers of TCP/IP choose a scheme analogous to physical network addressing in which each host on the Internet is assigned as 32-bit integer address called its ***Internet address*** or ***IP address.***

It is a unique number helps to identify each and every computer on Internet. IP addresses are in the format xxx.xxx.xxx.xxx, where each xxx is a number from 0 to 255. IP address is an identifier for a particular machine on a particular network. IP addresses are also referred to as IP numbers and Internet addresses. IP address consists of four sections separated by periods and each section has numbers from 0 to 255. These sections show machine itself or host both and the network that the host is on.

MSU Printer

The network portion of IP address is allocated to ISPs by internet... under the authority of IANA (Internet Assigned Numbers Authority). The... ISPs assign the host portion of IP address to the machines on networks th... operate. Which sections of IP address show the network and which sections... show the machine depend on the class of IP address, that is assigned to a... network.

There are five classes of IP addresses – Class A, Class B, Class C, Class... D, and Class E. The classes correspond either to the size of network (i.e.... number of hosts that the network can support) or are reserved of specific... purposes, such as multicasting and experimentation.

The example of class A, class B and class C IP addresses are compared... as –

Class A	**202**.0.0.0
Class B	**127.54**.0.0
Class C	**234.154.222**.0

Here, the bold numbers represent the network and the normal numbers... represent hosts on the network. Thus, the network of Class A can support... many more hosts than the network of Class C.

Class D is reserved for ***multicast addresses.*** Multicasting allows copies... of a datagram to passed to a select group of hosts rather than to an individual... host. Class E addresses are reserved for future use.

Each Internet address consists of four bytes (32 bits), defining three... fields – class type, netid, and hostid. These parts are of varying lengths... depending on the class of the address (see fig. 4.18).

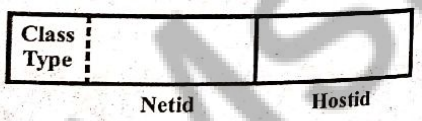


Fig. 4.18 Internet Address

The different classes are designed to cover the needs of different... types of organizations. For example, class A addresses are numerically the... lowest. They use only one byte to identify class type and netid, and leave... three bytes available for hostid numbers. This division means that class A... networks can accommodate for more hosts than can class B or class C... network which provide two-and one-byte hostid fields, respectively... Currently both class A and class B are full. Addresses are available in class... C only.

Fig. 4.19 shows the form of each IP address class.

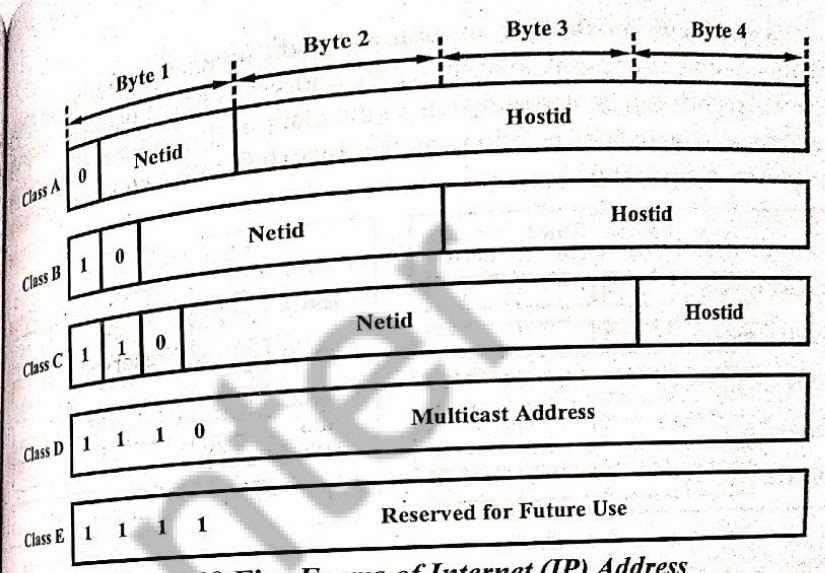


Fig. 4.19 Five Forms of Internet (IP) Address

Q.28. Write the advantages and disadvantages of IP address.

Ans. Some advantages are as follows –

(i) IP addresses are unique numbers, i.e., no two systems directly connected to the Internet can have the same IP address.

(ii) IP addresses are standardized and follow global conventions. All the networks that are given by Internet NIC under the authority of Internet Assigned Numbers Authority to the ISPs who allocate the host portion of the IP address to the machines that are connected to the network only. Only real Internet hosts IP addresses.

Some disadvantages are as follows –

(i) They are very difficult to remember and the possibility of committing an error is quite high.

(ii) We are running short of addresses as the network grow constantly.

(iii) If a computer is transferred from one place to another, it is quite possible its IP addresses will get modified thus causing inconvenience.

(iv) Routing problem has arisen because the number of resources on the Internet have increased and so has the data flow.

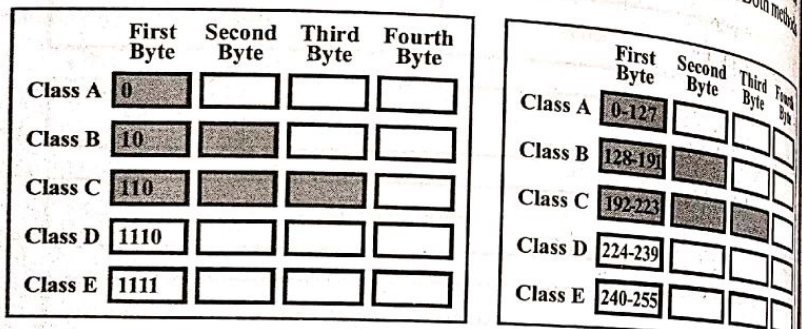
Q.29. Discuss classful addressing in brief.

Ans. IPv4 addressing, at its inception, used the concept of classes. This architecture is called ***classful addressing***.

In classful addressing, the address space is divided into five classes – A, B, C, D and E. Each class occupies some part of the address space.

MSInvertet

We can find the class of an address when given the address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few bits can immediately tell us the class of the address. If the address is given in decimal-dotted notation, the first byte defines the class. Both methods are shown in fig. 4.20.



(a) Binary Notation *(b) Dotted Decimal Notation*

Fig. 4.20 Finding the Classes in Binary and Dotted Decimal Notation

Classes and Blocks – One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size as shown in table 4.1.

Table 4.1 Number of Blocks and Block Size in Classful IPv4 Addressing

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

In classful addressing, a large part of the available addresses were wasted.

Q.30. How many host per network in each IP address class can exist? Show with example. *(R.G.P.V., June 2010)*

Ans. In classful IP addressing, an IP address in class A, B or C is divided into two parts – a network identification (netid) and a host identification (hostid). The netid identifies the network, and the hostid identifies the specific host on the designated network. The length of the netid and hostid vary, depending on the class of the address. With class A addresses, the first eight bits denote the netid, and the remaining 24 bits make up the hostid. With class B addresses, the first 16 bits represent the netid, and the remaining 16 bits identify the hostid. With class C addresses, the first 24 bits identify the netid, and the remaining eight bits make up the hostid.

In class A addresses, one byte defines the netid and the first bit must be 0. This means only seven bits for the netid. Therefore, the maximum number of class A network addresses is $2^7 = 128$. In class A addresses, there are 24 bits reserved for the host ID. Therefore, there are $2^{24} = 16777216$ host addresses possible for each class A network address. In class B addresses, two bytes define the netid and the first two bits must be 10. Therefore, the maximum number of class B network addresses is $2^{14} = 16384$. In class B addresses, two bytes defines the host ID. Therefore, there are $2^{16} = 65536$ host addresses possible for each class B network address. In class C addresses, three bytes define the network ID, and the first three bits must be 110. Therefore, the maximum number of class C network addresses is $2^{21} = 2097152$. In class C addresses, one byte defines the hostid. Therefore, the maximum number of host addresses possible for each class C address is $2^8 = 256$.

Q.31. Describe classless addressing.

Ans. To overcome address depletion and give more organizations access to the internet, classless addessing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

Address Blocks – In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a blcok (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity.

Restriction – To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks –

(i) The addresses in a block must be contiguous, one after another.

(ii) The number of addresses in a block must be a power of 2 (1,2,4,8,....).

(iii) The first address must be evenly divisible by the number of addresses.

Mask – A better way to define a block of addresses is to select any address in the block and the mask. A mask is a 32-bit number in which the n leftmost bits are 1s and the 32 – n rightmost bits are 0s. However, in classless addressing the mask for a block can take any value from 0 to 32. It is very convenient to give just the value of n preceded by a slash (CIDR notation).

The address and the */n* notation completely define the whole block (the first address, the last address and the number of addresses).

First Address – The first address in the block can be found by setting the 32 – n right-most bits in the binary notation of the address to 0s.

Last Address – The last address in the block can be found by setting the 32 – n right-most bits in the binary notation of the address to 1s.

Number of Addresses – The number of addresses in the block is the difference between the last and first address. It can easily be found using the formula 2^{32-n}.

Q.32. Differentiate between classful and classless addressing.

Ans. Difference between classful and classless addressing are as follows –

S.No.	*Classful Addressing*	*Classless Addressing*
(i)	In classful addressing, the concept of classes was used to designate the different type of addresses.	In classless addressing, there are no classes, but the address are still granted in blocks.
(ii)	Here the address space is divided in five classes namely, class A, B, C, D, and E. Each class occupies some part of address space.	It incorporates variable length blocks of IP addresses that essentially belongs to no class.
(iii)	In this addressing, a large part of the available addresses were wasted.	Classful addressing which is almost obsolete, is replaced with classless addressing.

Q.33. Differentiate logical, classful and classless addressing techniques. ***(R.G.P.V., June 2014)***

Ans. Refer the ans. of Q.26, Q.29, Q.31 and Q.32.

Q.34. Justify the need of logical addressing scheme in networking. Also, explain how a physical address is mapped into a logical address. ***(R.G.P.V., Dec. 2015)***

Ans. Communication at the network layer is host-to-host (computer-to-computer), a computer somewhere in the world needs to communicate with another computer somewhere else in the world. Usually, computers communicate through the Internet. The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer.

For this level of communication, we need a global addressing scheme and called as logical addressing. Logical address are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose.

Physical to Logical Address Mapping – There are occasions in which a host knows its physical address, but requires to know its logical address. This may happen in two cases –

(i) A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.

(ii) An organization does not have sufficient IP addresses to locate to every station, it requires to locate IP addresses on demand. The station can transmit its physical address and ask for a short time lease.

RARP, BOOTP and DHCP – The reverse address resolution protocol (RARP) permits a newly-booted workstation to broadcast its Ethernet address and say – My 48-bit Ehternet address is 14.04.05.18.01.25. Does anyone out there know my IP address ? The RARP server sees this request, looks up the Ethernet address in its configuration files, and sends back the corresponding IP address.

Using RARP is better than embedding an IP address in the memory image because it permits the same image to be used on all machines. If the IP address were buried inside the image, each workstation would need its own image.

A demerit of RARP is that it uses a destination address of all 1s to reach the RARP server. Although, such broadcasts are not forwarded by routers, so a RARP server is required on each network. To get around this problem, an alternative bootstrap protocol known as BOOTP was introduced. Unlike RARP, BOOTP uses UDP messages, which are forwarded over routers. It also gives a disklesss workstation with additional information, including the IP address of the file server holding the memory image, the IP address of the default router, and the subnet mask to use.

A disadvantage of BOOTP is that it needs manual configuration of tables mapping IP address to Ethernet address. When a new host is added to a LAN, it cannot use BOOTP until an administrator has assigned it an IP address and entered its into the BOOTP configuration tables by hand. To eliminate this error-prone step, BOOTP was extended and given a new name DHCP (dynamic host configuration protocol). DHCP permits both manual IP address assignment and automatic assignment.

Like RARP and BOOTP, DHCP is based on the idea of a special server that assigns IP addesses to hosts asking for one. This server require not be on the same LAN as the requesting host. Since the DHCP server may not be reachable by broadcasting, a DHCP relay agent is required on each LAN, as shown in fig. 4.21.

To find its IP address, a newly-booted machine broadcasts a DHCP discover packet. The DHCP relay agent on its LAN intercepts all DHCP broadcasts. When it finds a DHCP discover packet, it sends the packet as a unicast packet to

the DHCP server, possibly on a distant network. The only piece of information the relay agent needs is the IP address of the DHCP server.

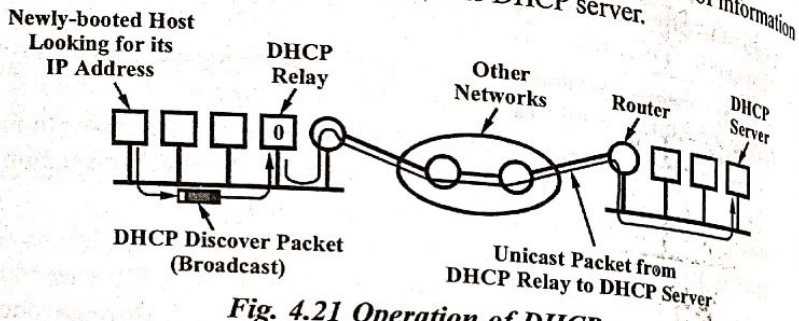


Fig. 4.21 Operation of DHCP

An issue that occurs with automatic assignment of IP addresses from a pool is how long an IP address should be allocated. If a host leaves the network and does not return its IP address to the DHCP server, that address will be permanently lost. After a period of time, many addresses may be lost. To prevent that from happening, IP address assignment may be for a fixed period of time, a method known as ***leasing***. Just before the lease expires, the host must ask the DHCP for a renewal. If it fails to make a request or the request is denied, the host may no longer use the IP address it was given earlier.

Q.35. What is packet forwarding ?

Or

Explain the term forwarding.

Ans. Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination. However, this simple solution is impossible today in an internetwork such as the Internet because the number of entries needed in the routing table would make table lookups inefficient.

Q.36. Describe several packet forwarding techniques.

Ans. Several forwarding techniqu es can make the size of the routing table manageable and also handle issues such as security. We briefly discuss these methods below.

Next-hop Method versus Route Method – One technique to reduce the contents of a routing table is called the ***next-hop method***. In this technique, the routing table holds only the address of the next hop instead of information about the complete route ***(route method)***. The entries of a routing table must be consistent with one another. Fig. 4.22 shows how routing tables can be simplified by using this technique.

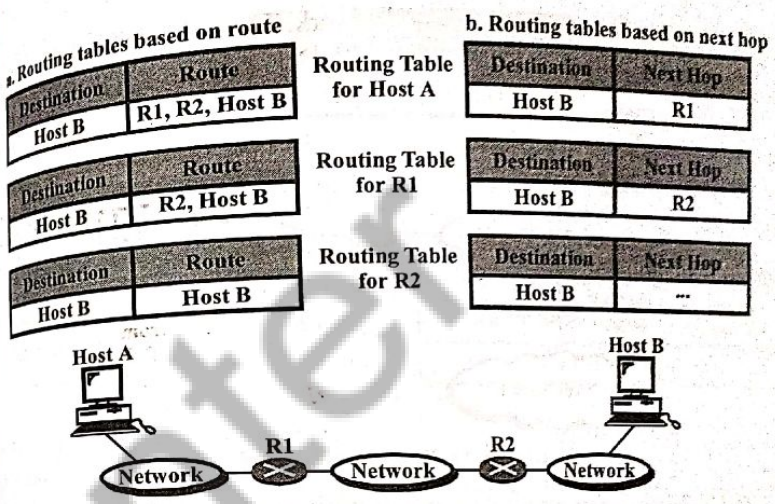


Fig. 4.22 Route Method versus Next-hop Method

Network-specific Method versus Host-specific Method – A second technique to reduce the routing table and simplify the searching process is called the ***network-specific method***. Here, instead of having an entry for every destination host connected to the same physical network ***(host-specific method)***, we have only one entry that defines the address of the destination network itself. In other words, we treat all hosts connected to the same network as one single entity. Fig. 4.23 shows the concept. Host-specific routing is used for purposes such as checking the route or providing security measures.

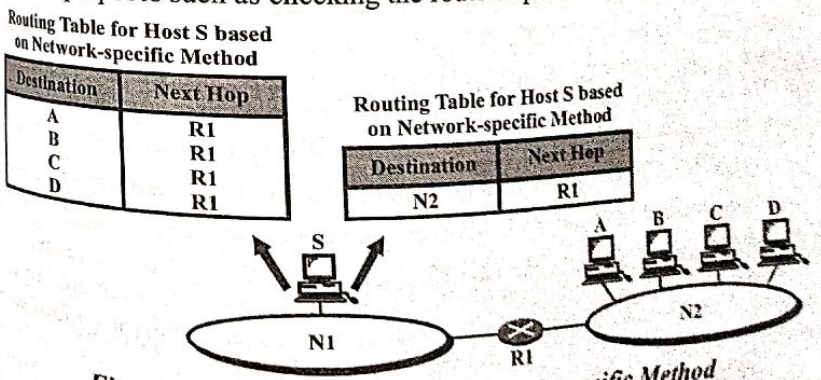


Fig. 4.23 Host-specific versus Network-specific Method

Default Method – Another technique to simplify routing is called the ***default method***. In fig. 4.24 host A is connected to a network with two routers. Router R1 routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the default (normally defined as network adress 0.0.0.0).

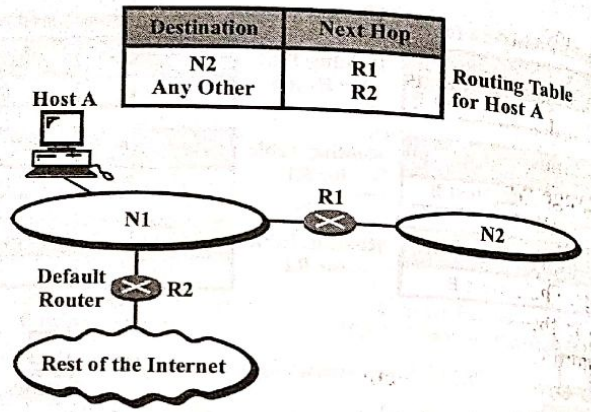


Fig. 4.24 Default Method

Q.37. Write short note on fragmentation and reassembly.

Ans. Fragmentation is the division of a datagram into smaller units to accommodate the MTU (maximum transfer unit) of a data link protocol. The designers decided to make the maximum length of the IPv4 datagram equal to 65535 bytes to make the IPv4 protocol independent of the physical network. When we use a protocol with an MTU of this size, this makes transmission more efficient. However, we should divide the datagram to make it possible to pass through these networks for other physical networks. This is known as fragmentation. A datagram may be fragmented by the source host or any router in the path but there is a tendency to limit fragmentation only at the source. The reassembly of the datagram is done only by the destination host because each fragment becomes an independent datagram. So it is logical to do the reassembly at the final destination. An even stronger objection to reassembling packets during the transmission is the loss of efficiency it incurs.

Q.38. Write introductory note on ICMP. Also give ICMP messages format.

Ans. As we know that the IP gives connectionless and unreliable datagram delivery. It was made this way to make maximum use of network resources. A datagram from its original source to its final destination is delivered by IP protocol which is a best-effort delivery service. But lack of error control and lack of assistance mechanisms are the two drawbacks.

The IP protocol has no error-reporting or error-correcting mechanism. What happens if a router must discard a datagram because it cannot find a router to the final destination, or because the time-to-live field has a zero value ? What happens when something goes wrong ? What happens when the final destination host must discard all fragments of a datagram because it has not obtained all fragments within a predetermined time limit ? These are the conditions where an error has obtained and IP protocol has no built in mechanism to get the original host.

The IP protocol also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router or another host is alive. Sometimes a network administrator needs information from another host or router. The ICMP has been designed to compensate for the two above drawbacks.

An ICMP message has an 8 byte header and a variable size data section. For each message type general format of header is different but first 4 bytes are common to all. Fig. 4.25 shows the general format of ICMP messages.

In fig. 4.25, type defines the type of the message. The code field specifies the reason for the specific message type. For obtaining the original packet which had the error, the data section in error messages carries information. The data section carries additional information depend on the type of the query in query messages.

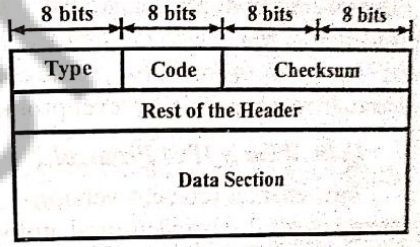


Fig. 4.25

Q.39. Explain Internet Protocol (IP). Also show its position in TCP/IP protocol suite with the help of diagram.

Ans. The Internet Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless datagram protocol - a best-effort delivery service. The term best-effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. Fig. 4.26 shows the position of IP in the TCP/IP suite.

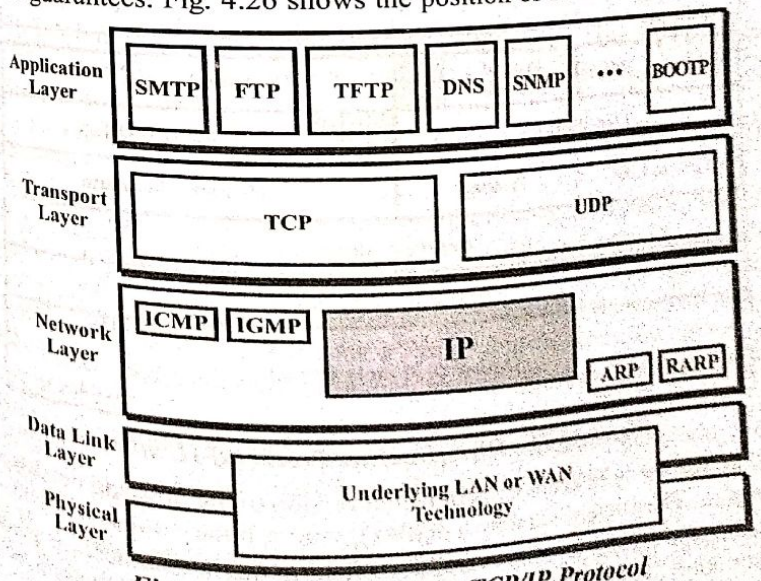


Fig. 4.26 Position of IP in TCP/IP Protocol

If reliability is important, IP must be paired with a reliable protocol such as TCP. An example of more commonly understood best-effort delivery service is the post office. The post office does its best to deliver the mail but does not always succeed. If an unregistered letter is lost, it is upto the sender or would be recipient to discover the loss and rectify the problem.

IP is also a connectionless protocol packaged for a packet switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order. Also, some could be lost or corrupted during transition. Again, IP relies on a higher level protocol to take care of all these problems.

Q.40. What is IPv4 Protocol ? ***(R.G.P.V., June 2015)***

Ans. Internet protocol version 4 (IPv4) is the fourth generation of the Internet protocol. It is widely used protocol in data communication over different types of networks. This protocol is a connectionless protocol employed in packet-switched layer networks like Ethernet. It provides the logical connection between network devices by providing identification for each device.

Q.41. What do you mean by datagram ? Give a brief description of each field of IPv4 datagram.

Ans. Packets in the IPv4 layer are known as datagrams. An IP datagram consists of a header part and text part. The header has a 20-byte fixed part and a variable length optional part. Fig. 4.27 shows the IPv4 header format.

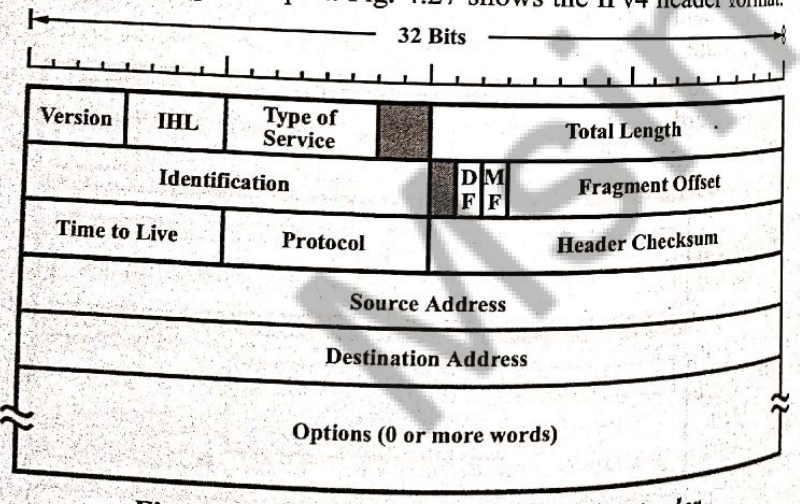


Fig. 4.27 The IPv4 (Internet Protocol) Header

The Version field keeps track of which version of the protocol the datagram belongs to. The current version is 4(IPv4), with a binary value of 0100.

Since the header length is variable, a field in the header, IHL, is given to tell how long the header is, in 32-bit words. The minimum value is 5, which

applies when no options are present. The maximum value of this 4-bit field is 15, which limits the header to 60 bytes, and thus the options to 40 bytes.

The Type of Service field is one of the few fields that has changed its meaning over the years. It was and is still intended to distinguish between different classes of service. Several combinations of reliability and speed are possible. For digitized voice, fast delivery beats accurate delivery. For file transfer, error-free transmission is more important than fast transmission.

Originally, the 6-bit field contained (from left to right), a three-bit Precedence field and three flags, delay, throughput, and reliability. The Precedence field was a priority, from 0 to 7. The three flag bits permitted the host to specify what it cared most about from the set.

The Total Length includes everything in the datagram-both header and data. The maximum length is 65,535 bytes.

The identification field is required to allow the destination host to determine which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same identification value.

Next comes an unused bit and then two 1-bit fields. DE starts for don't fragment. It is an order to the routers not to fragment the datagram because the destination is incapable of putting the pieces back together again.

MF stands for more fragments. All fragments except the last one have this bit set. It is required to know when all fragments of a datagram have arrived.

The Fragment Offset is a pointer that defines the offset of the data in the original datagram.

The Time to live field shows the number of hops a datagram can travel before it is discarded. The source host sets this field to an initial valve, when it creates the datagram.

The Protocol field defines which upper-layer protocol data are encapsulated in the datagram.

Header checksum verifies the header only. Such a checksum is useful for detecting errors generated by bad memory words inside a router. The algorithm is to add up all the 16-bit halfwards as they arrive, using one's complement arithmetic and then take the one's complement of the result. For purposes of this algorithm, the Header checksum is assumed to be zero upon arrival.

The Source address and Destination address show the network number and host number.

The Options field provides more functionality to the IP datagram. It can carry fields that are security, strict source routing, loose source routing, record route and timestamp.

Q.42. Explain the frame format of IPv4. ***(R.G.P.V., June 2017)***

Ans. Refer the ans. of Q.41.

Q.43. Describe the reasons for developing IPv6.

Ans. The original network-layer protocol in the TCP/IP protocol suite is Internetwork protocol, version 4 (IPv4), which was designed to provide host-to-host communications across the Internet. However, the Internet has changed significantly since its inception in the early 1970s, leaving IPv4 with several inherent shortcomings, such as following –

(i) Limited number of IP addresses.

(ii) Inefficient use of IP addresses.

(iii) Inadequate delay and resource reservation strategies for real-time audio and video transmission.

(iv) No provisions for encryption or decryption.

(v) No provision for authentication.

(vi) Inefficient provisions for routing.

(vii) Inefficient use of options.

(viii) Inadequate type options.

To overcome the shortcomings of IPv4, the Area Directors of the Internet Engineering Task Force at the Toronto IETF meeting on July 25, 1994, created a new generation of IP addressing called Internet Protocol version 6 (IPv6), which is sometimes called IPng (IP next generation).

IPv6 was designed as an evolutionary and radical progression from IPv4. IPv6 can be installed as a normal software upgrade in the Internet devices, as it is interoperable with the current IPv4. The deployment strategy for IPv6 is designed for immediate implementation, which is possible because IPv6 is flexible and capable of running on high performance networks, such as ATM, and at the same time efficient enough to be used on low-bandwidth networks, such as wireless.

Q.44. Explain IPv4 header format with the help of a neat diagram. State four major improvements of IPv6 over IPv4. ***(R.G.P.V., Dec. 2014)***

Ans. **IPv4 Header Format** – Refer the ans. of Q.41.

IPv6 has following advantages (enhancements) over IPv4 –

(i) Expanded Address Space – IPv6 uses 128-bit addresses instead of the 32-bit addresses of IPv4. This is an increase of address space by a factor of 2^{96}. It has been pointed out that this allows on the order of 6×10^{23} unique addresses per square meter of the surface of the earth. Even if addresses are very inefficiently allocated, this address space seems secure.

(ii) Improved Option Mechanism – IPv6 options are placed in separate optional headers that are located between the IPv6 header and the transport layer header. Most of these optional headers are not examined or processed by any router on the packet's path. This simplifies and speeds up router processing of IPv6 packets compared to IPv4 datagrams. It also makes it easier to add additional options.

(iii) Address Autoconfiguration – This compability provides for dynamic assignment of IPv4 addresses.

(iv) Increased Addressing Flexibility – IPv6 includes the concept of anycast address, for which a packet is delivered to just one of a set of nodes. The scalability of multicast routing is improved by adding a scope field to multicast addresses.

(v) Support for Resource Allocation – Instead of the type-of-service field in IPv4, IPv6 enables the labeling of packets belong to a particular traffic flow for which the sender requests special handling. This aids in the support of specialized traffic such as real-time video.

(vi) Support for More Security – The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

(vii) Better Header Format – IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

Q.45. Explain the salient features of IPv6. ***(R.G.P.V., May 2019)***

Ans. Some of the salient features of IPv6 are as follows –

(i) Resource Allocation – IPv6 supports resource allocation by adding the mechanism of flow label. A transmitter can request special handling of the packet in the Internet by using flow label.

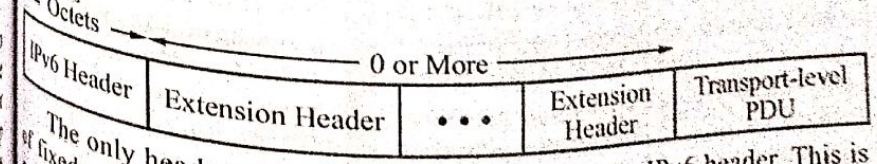
(ii) Address Space – An IPv6 address is 128 bits long, which can effectively handle the problems generated by a limited IPv4 address space.

(iii) Support for Security – IPv6 supports encryption and decryption options, which give authentication and integrity.

(iv) Modified Header Format – IPv6 separates options from the base header. This helps speed up the routing process since most of the options need not be checked by routers.

Q.46. Discuss the IPv6 structure in brief.

Ans. An IPv6 protocol data unit (known as a packet) has the following general form –



The only header that is referred to simply as the IPv6 header. This is of fixed size with a length of 40 octets compared to 20 octets for the mandatory portion of the IPv4 header. The following extension headers have been defined –

(i) Hop-by-Hop Options Header – Defines special options that require hop-by-hop processing.

(ii) Routing Header – Provides extended routing, similar to IPv4 source routing.

(iii) Fragment Header – Contains fragmentation and reassembly information.

(iv) Authentication Header – Provides packet integrity and authentication.

(v) Encapsulating Security Payload Header – Provides privacy.

(vi) Destination Options Header – Contains optional information to be examined by the destination node.

The IPv6 standard recommends that, when multiple extension headers are used, the IPv6 headers appear in the following order.

(i) IPv6 header – Mandatory must always appear first

(ii) Hop-by-Hop options header

(iii) Destination options header – For options to be processed by the first destination that appears in the IPv6 Destination Address field plus subsequent destinations listed in the routing header

(iv) Routing header (v) Fragment header (vi) Authentication header

(vii) Encapsulating security payload header

(viii) Destination option header for options to be processed only by the final destination of the packet.

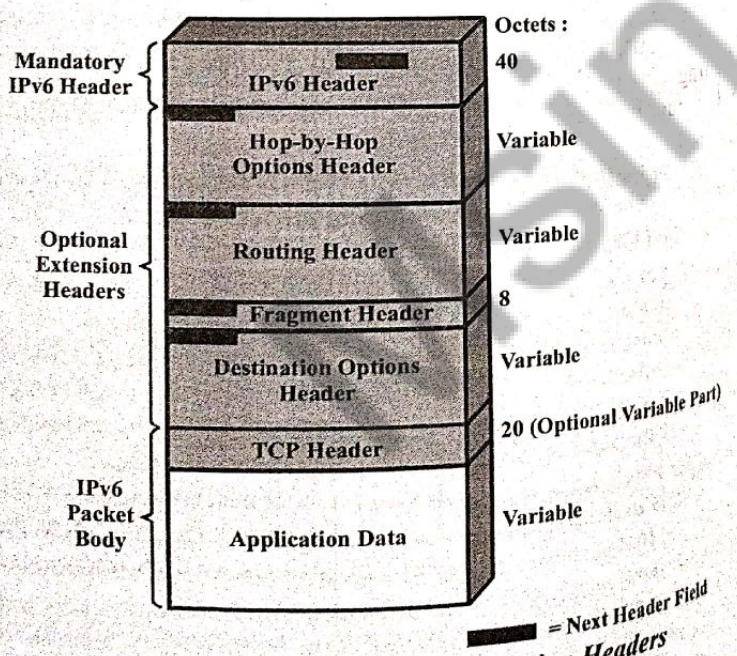


Fig. 4.28 IPv6 Packet with Extension Headers

Fig. 4.28 shows an example of an IPv6 packet that includes an instance of each header, except those related to security.

Note that the IPv6 header and each extension header include a Next Header field. This field identifies the type of the immediately following header. If the next header is an extension header, then this field contains the type identifier of that header. Otherwise, this field contains the protocol identifier of the upper-layer protocol using IPv6 (typically a transport-level protocol), using the same values as the IPv4 protocol field. In fig. 4.28, the upper-layer protocol is TCP, so that the upper-layer data carried by the IPv6 packet consist of a TCP header followed by a block of application data.

Q.47. How can you compare IPv4 and IPv6 ? (R.G.P.V., June 2010, 2011)

Or

Write the difference between IPv4 and IPv6. (R.G.P.V., Dec. 2012)

Or

Give a comparative study of IPv4 and IPv6. (R.G.P.V., June 2014)

Ans. **Comparison between IPv4 and IPv6 –**

S.No.	IPv4	IPv6
(i)	Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
(ii)	IP_{sec} support is optional.	IP_{sec} support is required.
(iii)	IPv4 header does not identify packet flow for QoS handling by routers.	IPv6 header contains flow label field, which identifies packet flow for QoS handling by router.
(iv)	Both routers and the sending host fragment packets.	Only the sending hosts fragment packets; routers do not.
(v)	Header includes a checksum.	Header does not include a checksum.
(vi)	Header includes options.	All optional data is moved to IPv6 extension headers.
(vii)	Internal Group Management Protocol (IGMP) manages membership in local subnet groups.	Multicast listener discover (MLD) messages manage membership in local subnet groups.
(viii)	Broadcast addresses are used to send traffic to all nodes on a subnet.	IPv6 uses a link-local scope all-nodes multicast addresses.
(ix)	Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
(x)	Uses host address (A) resource records in domain name system (DNS) to map host names to IPv4 addresses.	Uses host addresses (AAAA) resource records in DNS to map host names to IPv6 addresses.
(xi)	Must support a 576 byte packet size (possibly fragmented).	Must support a 1280 byte packet size (without fragmentation).

Q.48. What are the limitations of IPv4 ? Compare IPv4 and IPv6. *(R.G.P.V., June 2012)*

Ans. Refer the ans. of Q.43 and Q.47.

NUMERICAL PROBLEMS

Prob.3. A host in an organization has an IP address 150.37.64.34 and a subnet mask 255.255.240.0. What is the address of this subnet ? What are the ranges of IP address that is host can have on this subnet ? *(R.G.P.V., June 2012, Dec. 2015)*

Sol.

IP address (decimal)	150	37	64	34
IP address (binary)	10010110.	00100101.	01000000.	00100010
Subnet mask (binary)	11111111.	11111111.	11110000.	00000000
Result of ANDing	10010110.	00100101.	01000000.	00000000
Subnet Address	150	37	64	0

Subnet Address = 150.37.64.0

Ranges of IP Address – To find the ranges of IP address, first of all we find the first and last addresses of this subnet.

Then first address is obviously the subnet address and it is given by 150.37.64.0.

For deriving the last address we can make rightmost 32 – 20 = 12 bits in the binary notation of the address to 1s.

Thus,

First IP address : 10010110.00100101.01000000.00000000

Last IP address : 10010110.00100101.01001111.11111111

(150.37.79.255)

The number of addresses for subnetwork can be found by counting the number of 0s in the subnet mask.

∵ Number of 0s in subnet mask = 12

∴ Number of addresses per subnet = $2^{12} = 4096$

150.37.64.0 ----------150.37.64.255

150.37.65.0 ----------150.37.65.255

150.37.66.0 ----------150.37.66.255

.

.

.

150.37.79.0 ----------150.37.79.255

UNIT 5

TRANSPORT AND APPLICATION LAYERS

TRANSPORT LAYER – DESIGN ISSUES, UDP – HEADER FORMAT, PER-SEGMENT CHECKSUM, CARRYING UNICAST/MULTICAST REAL-TIME TRAFFIC

Q.1. What do you understand by transport layer ?

Ans. Transport layer is situated between the network layer and the session layer of an end system. Transport layer is implemented only in the end systems where the applications are implemented, while the network layer and the other lower layers reside in all the end systems and intermediate systems. Interactions between peer transport layers are end-to-end. These are made possible by the data transfer service provided by the network layer. Like other OSI layers, transport layer is defined by the service it provides to the users that are the session entities and by the transport layer protocol that is used by the transport entities to provide the service.

Q.2. What is the purpose of transport layer ?

Ans. Transparent, reliable and cost effective transfer of a data between the user entities in the session layers is made possible by the transport layer. Transparency implies that the transport entities do not place and constraints on the content of the data units received from the user entities. Reliable means that the data units are received as they are transmitted by the user entities. When any kind of error takes place during the transfer, an indication is given to the receiver. Cost effectiveness means that the underlying network service is utilized in the most optimum manner to provide the quality of service requested by the user entities.

Q.3. Discuss the design issues of transport layer.

Ans. The issues involved in the design of transport layer are as follows –

(i) Addressing – When an application process wants to setup a connection to a remote application process, it must specify a valid transport address. The addressing method must be helpful for the transport layer entities to use the available network addresses. A special process known as name

server or directory server is used for providing addresses for the required service name. Whenever a new service is created, it must register itself with the name server. The name server maintains an internal database in which this information is added. The addressing method is hierarchical so that the transport entity will be able to locate the machine easily.

(ii) Connection Establishment and Release – Transport Protocol Data Unit (TPDU) is the data unit for the transport layer similar to packets of the network layer and frames of the data link layer connection request and connection accepted TPDU are interchanged to establish a connection. When the transmitted units get timeout and retransmitted a number of times, it increases the number of units in the network. This problem usually arises in datagram networks when different packets are routed through different routes. Hence, it is needed to restrict the packet lifetime to avoid duplication.

There are two ways to release connections – symmetric and asymmetric release. In asymmetric release, if connection on one side is released the other side is also released automatically. In symmetric release, both the ends demand for a separate release. The main issue in asymmetric release is data loss due to abrupt release. Symmetric release also suffers from a similar problem. The transport layer protocol must be designed to make efficient and reliable connections and releases.

(iii) Connection Management – The two main issues in the connection management are flow control and buffering. The flow control techniques are used to prevent slow receiving ends from fast senders. Buffering is used to offer reliability at the transport layer level, when the network layer is unreliable.

(iv) Multiplexing – There are situations in which several transport connections share a single network connection. Multiplexing provides a good way for maintaining uniform transmission time to all connections.

(v) Crash Recovery – Recovery from host or router crash is a serious issue. For transport entities using virtual circuits, recovery from router failure can be done by establishing the circuit again and retransmitting the packet that is not received. If datagram service is used, recovery from router failure is done by tracing out the sequence numbers of missed packets and retransmitting them. Host failure is a serious issue and is to be handled. Identification of failed host, intimating other hosts about the failure, and recovering status just before the crash are big problems.

Q.4. Write short note on UDP. ***(R.G.P.V., June 2011)***

Or

Explain the working of user datagram protocol. ***(R.G.P.V., Dec. 2014)***

Ans. UDP (user datagram protocol) is another transport layer protocol that is a part of TCP/IP suite. It is an unreliable, connectionless protocol that does not guarantee delivery and duplicate protection. UDP is basically just IP with a short header added. It provides non-sequential transport functionality when reliability and security are less important than size and speed.

UDP provides a way for applications to send encapsulated raw IP datagrams without establishing any connection. UDP is more appropriate than TCP in some contexts; like it is more robust at lower layers. UDP has very little to do. Mainly, it adds a port addressing capability to IP. Since its header is shorter, it involves less overheads.

UDP is used by the applications that do not want TCP's sequencing and flow control and wish to provide their own. It is widely used for one-shot, client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. Thus, there is a place at the transport layer for both connection-oriented and connectionless type of service. UDP is described in RFC 768.

UDP provides a connectionless service for application-level procedures. Therefore, UDP is an unreliable service. However, the overhead of the protocol is low, which may be enough in several cases. An example of the use of UDP is in the context of network management.

The relation of IP, TCP, and UDP is shown in fig. 5.1.

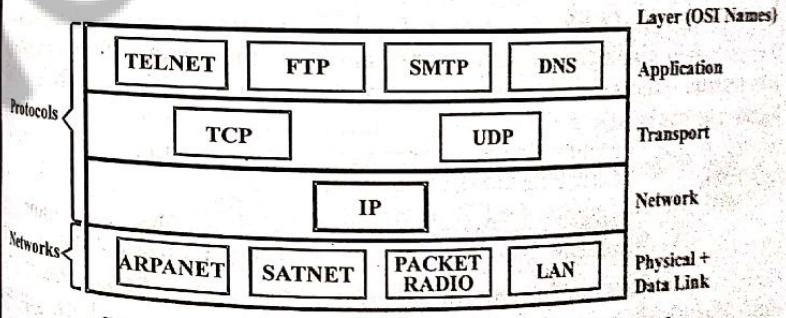


Fig. 5.1 Protocols and Networks in TCP/IP Model

Q.5. What is UDP ? In case where reliability is not a primary importance, UDP would make a good transport protocol. Give example of specific case. ***(R.G.P.V., June 2012)***

Or

In cases where reliability is not a primary importance. UDP would make a good transport protocol. Give examples of specific cases. ***(R.G.P.V., Dec. 2016)***

Ans. **UDP** – Refer the ans. of Q.4.

Transmission Control Protocol (TCP) provides a connection-oriented user-to-user byte stream service. This means it provides a logical connection between two sites and is capable of transmitting a sequence of bytes between them. TCP is a reliable protocol that provides flow control, error control, loss control

and sequencing. TCP provides guaranteed data transfer. If in TCP, where reliability is not of primary importance, then UDP would make a good transport protocol because UDP is preferred when speed and size is more important. UDP is simpler than TCP since its header is shorter than TCP header and thus involves less overhands.

FTP, TFTP and NFS are protocols of TCP. In FTP, File Transfer Protocol is the standard mechanism provided by TCP/IP for copying a file from one host to another. Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment.

Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. FTP offers many facilities beyond the transfer function itself.

(i) Interactive Access – Although FTP is designed to be used by programs, most implementations provides an interactive interface that allows humans to easily interact with remote servers.

(ii) Format (Representation) Specification – FTP allows the client to specify the type and format of stored data. For example, the user can specify whether a file contains text or binary integers and whether text files use the ASCII or EBCDIC character sets.

(iii) Authentication Control – FTP requires clients to authorize themselves by sending a login name and password to the server before requesting file transfer. The server refuses access to clients that cannot supply a valid login and password.

Q.6. What are the advantages of UDP ?

Ans. The advantages of UDP are as follows –

(i) Simplicity – For the network not for the programmer.

(ii) Does not Include the Overhead Needed to Detect Reliability and Maintain Connection Oriented Semantics – UDP packets require considerably less processing at the transmitting and receiving hosts.

(iii) Less Heavy to Manage for the OS – Many operating systems impose limits on how many simultaneous TCP/IP connections they can support.

Q.7. What are the uses of UDP ?

Ans. Some of the uses of the UDP protocol are given below –

(i) UDP is suitable for a process with internal flow and error control mechanisms. For example, TFTP (Trivial File Transfer Protocol) process includes flow and error control. It can easily use UDP.

(ii) UDP is appropriate for a process which needs simple request-response communication with little concern for flow and error control. Generally, it is not used for a process which requires to transmit bulk data such as FTP.

(iii) UDP is used for management processes like SNMP.

(iv) UDP is used for some route updating protocols such as routing information protocol (RIP).

(v) UDP is suitable transport protocol for multicasting and broadcasting. These facilities are built in the UDP software but not in the TCP software.

Q.8. Why is UDP needed ? Why can't user program directly access IP ? ***(R.G.P.V., Dec. 2017)***

Ans. Refer the ans. of Q.7.

Applications cannot access IP directly due to lack of application level (port) addressing. UDP adds a port addressing capability to IP. It also includes an optional checksum for the user data which provides error checking.

Q.9. Give the format of UDP datagram. ***(R.G.P.V., June 2017)***

Or

Write short note on UDP header format. ***(R.G.P.V., June 2014)***

Or

Explain the header format of UDP protocol. ***(R.G.P.V., Dec. 2015)***

Or

Write short note on packet format of UDP. ***(R.G.P.V., May 2018)***

Ans. UDP packets, called user datagrams, have a fixed-size header of 8 bytes. The format of a user datagram is shown in fig. 5.2.

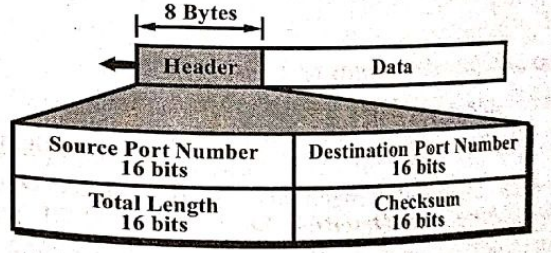


Fig. 5.2 User Datagram Format

The fields are as follows –

(i) Source Port Number – This is the port number used by the process running on the source host. It is 16 bits long. It means that the port number can range from 0 to 65, 535. In most cases, if the source host is the client, the port number is an ephemeral port number requested by the process and selected by the UDP software running on the source host. In most cases, the port number is a well-known port number if the source host is the server (a server sending a response).

(ii) Destination Port Number – It is also 16 bits long. This is the port number used by the process running-on the destination host. In most cases, the port number is a well known port number when the destination host

is the server (a client sending a request) and the port number is an ephemeral port number when the destination host is the client (a server sending a response). For such a case, the server copies the ephemeral port number it has received in the request packet.

(iii) Length – This is a 16-bit field which defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. However, because a UDP user datagram is stored in an IP datagram with a total length of 65,535 bytes, the total length needs to be much less.

In a UDP user datagram, the length field is actually not essential. In an IP datagram a user datagram is encapsulated. In IP datagram, there is a field which defines the total length and there is another field that defines the header length. So we can deduce the length of a UDP datagram which is encapsulated in an IP datagram when we subtract the value of the second field from the first.

UDP length = IP length – IP header's length

(iv) Checksum – It is 16 bits long. This field is used to detect errors over the entire user datagram.

Q.10. Explain per-segment checksum error control in UDP.

Ans. In addition to the port numbers, the UDP header also gives a 16-bit checksum field for checking on the integrity of each datagram. Since the checksum computation for a UDP datagram is optional, it can be disabled by setting the checksum field to zero. The sender generates the checksum value and fills in the checksum field, which is to be verified by the receiver. The receiver recalculates the checksum with the received datagram and verifies if the result matches the value stored in the UDP checksum field to ensure that each received datagram is exactly the same as the one sent by the sender. UDP receivers will drop the datagrams whose checksum field does not match the result they have calculated. This mechanism ensures per-segment data integrity but not per-segment data reliability.

The UDP checksum field can store the 1's complement of the sum of all 16-bit words in the header and payload. Its calculation is same as IP checksum calculation. If a UDP datagram has an odd number of octets to be check-summed, the last octet is padded at the end with zero bits to make a 16-bit word for checksum computation. It is noted that the pad is not transmitted as part of the datagram because the checksum verification at the receiver follows the same padding procedure. The checksum also covers a 96-bit pseudo header, composed of four fields in the IP header – the source IP address, the destination IP address, protocol, and length. Checksum covering the pseudo header enables the receiver to detect the datagrams with incorrect delivery, protocol, or length information. For the case that the checksum computation results in zero, 0xFFFF is filled into the field.

UDP checksum is optional. However, it is highly recommended because some link protocols do not perform error control. When implementing UDP over IPv6, checksum becomes mandatory as IPv6 does not provide checksum at all. UDP checksum is omitted only for some real-time applications where latency and jitter between the application processes are more critical than error control.

Q.11. Discuss the role of UDP in carrying unicast/multicast real-time traffic.

Ans. Due to its simplicity, UDP is an appropriate carrier for unicast or multicast real-time traffic. This is because real-time traffic has the following properties: (i) it does not need per-flow reliability (retransmitting a lost real-time packet could be meaningless because the packet might not arrive in time), and (ii) its bit rate (bandwidth) relies mainly on the selected codec and is unlikely to be flow controllable. These two properties simplify the transport layer for real-time traffic to provide the addressing service only.

However, in addition to the basic process-to-process communication service, real-time applications also need additional services, which are synchronization between audio and video streams, data compression and decompression information, and path quality statistics. These services are mostly provided by the RTP.

TCP – CONNECTION MANAGEMENT, RELIABILITY OF DATA TRANSFERS, TCP FLOW CONTROL, TCP CONGESTION CONTROL, TCP HEADER FORMAT, TCP TIMER MANAGEMENT

Q.12. Write short note on TCP. ***(R.G.P.V., June 2011)***

Or

Explain how message exchange takes place between machine A and B using TCP connection. ***(R.G.P.V., Dec. 2014)***

Ans. Transmission control protocol (TCP) provides a connection-oriented user-to-user byte stream service. This means it provides a logical connection between two sites and is capable of transmitting a sequence of bytes between them. It divides a byte stream into a sequence of segments and sends them to the destination via a variation on a sliding window flow control protocol. It provides the initial handshaking by establishing, maintaining, and releasing connections. It handles requests to deliver information to a destination reliably, an important consideration since the lower layer does not guarantee about delivery of packets. TCP receives data the requests from its user, stores it in a TCP segment format and gives it to the IP, which is shown in fig. 5.3. It plays no role in the subsequent routing and transfer of information.

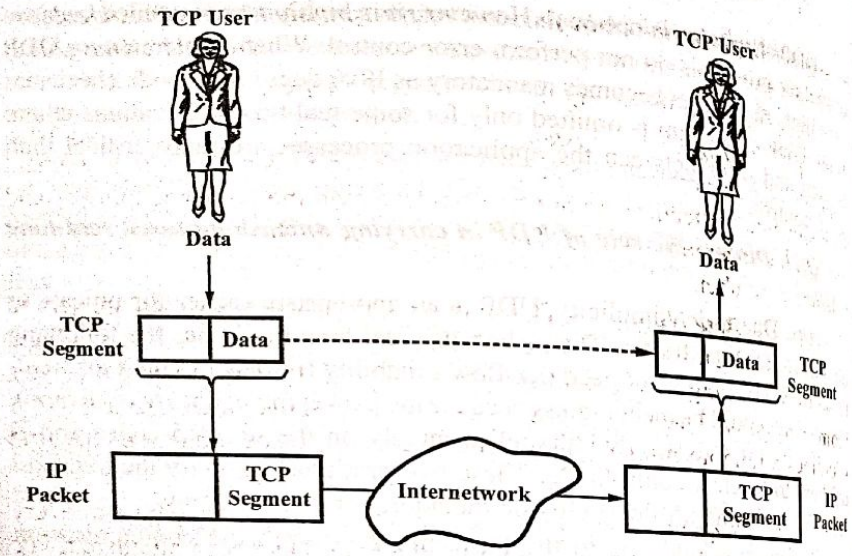


Fig. 5.3 TCP as a User-to-user Service

Each byte on a TCP connection has its own 32-bit sequence number. In case of a host blasting away at full speed on a 10 Mbps LAN, theoretically the sequence numbers could wrap around in an hour, but practically it takes much longer. Sequence numbers are used both for acknowledgement and for the window mechanism, in which separate 32-bit header fields are used.

Q.13. What is the difference between TCP and UDP ?
(R.G.P.V., June 2016)

Or

Differentiate between TCP and UDP. ***(R.G.P.V., Dec. 2017)***

Ans. The points of differentiation between TCP and UDP are as follows –

(i) TCP is a reliable connection-oriented protocol that provides flow control, error control, loss control and sequencing. While UDP is an unreliable connection-less protocol that provides no sequencing of data, error control and loss control.

(ii) TCP provides guaranteed data transfer while UDP gives no guarantee.

(iii) TCP is slower than UDP since there is no connection establishment and termination of circuit required in UDP.

(iv) UDP is simpler than TCP since its header is shorter than TCP header and thus involves less overheads.

(v) TCP is preferred when reliability and security is more important while UDP is preferred when speed and size is more important.

Q.14. Explain the main features of transmission control protocol.
(R.G.P.V., Dec. 2012)

Ans. There are following features of TCP as given below –

(i) Numbering System – The TCP software track of the segments being sent or received, in the segment header, there is no field to a segment number value. Instead, there are two fields known the sequence number and the acknowledgement number. These fields refer to the byte number and not a segment number.

(ii) Byte Number – TCP numbers all data bytes which are sent in a connection. Numbering is not dependent in every direction. It stores them in the transmitting buffer and numbers then, if TCP receives data bytes from a process. The numbering does not essentially begin from 0. TCP produces a random number between 0 to $2^{32} - 1$ to the number of the first byte.

(iii) Sequence Number – TCP assigns a sequence number to every segment which is being transmitted after the bytes have been numbered. For each segment, the sequence number is the number of the first byte carried in that segment.

(iv) Acknowledgement Number – The acknowledgement number defines the number of the next byte which the party expects to get. Furthermore, the acknowledgement number is comulative, it means that the party takes the number of the last byte which it has received safe and sound, add 1 to it, and announces this sum as the acknowledgement number.

(v) Error Control – TCP implements an error control mechanism to provide reliable service. Thus error control assumes a segment as the unit of data for error detection, error control is byte-oriented.

(vi) Flow Control – Unlike UDP, flow control is provided by TCP. The receiver of data controls the data amount which are to be transmitted via the transmitter. This can be performed to prevent the receiver from being overwhelmed with data. To use a byte oriented flow control, the numbering system permits TCP.

(vii) Congestion Control – TCP takes into account congestion in the network. The data amount transmitted via a transmitter is not only handled through the receiver, but is also computed by the congestion level in the network.

Q.15. The maximum payload of a TCP segment is 65,515 bytes. Why such a strange number chosen ? ***(R.G.P.V., June 2016)***

Ans. The entire TCP segment must fit in the 65,515 byte payload field of the IP packet. Since the TCP header is a minimum of 20 bytes, only 65,515 bytes are left over for TCP data.

Q.16. Give the advantages of RPC on UDP over transactional TCP. ***(R.G.P.V., June 2016)***

Ans. RPC need not use UDP packets, but RPC and UDP are a good fit and UDP is commonly used for RPC. However, when the operation requested is not idempotent (i.e., cannot be repeated safely, such as when incrementing a counter) or when the results/parameters may be larger than the maximum UDP packet, it may be necessary to set up a connection and send the request over it rather than use UDP.

Q.17. How connection is established and terminated in TCP using three way handshaking mechanism ? Describe in detail. ***(R.G.P.V., June 2015)***

Or

With neat diagram explain the process of connection establishment and release using 3-way handshaking in transport layer. ***(R.G.P.V., Dec. 2015)***

Ans. **TCP Connection Establishment** – Connections are established in TCP using the three-way handshake. To establish a connection, one side, let the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either specifying a specific source or nobody in particular.

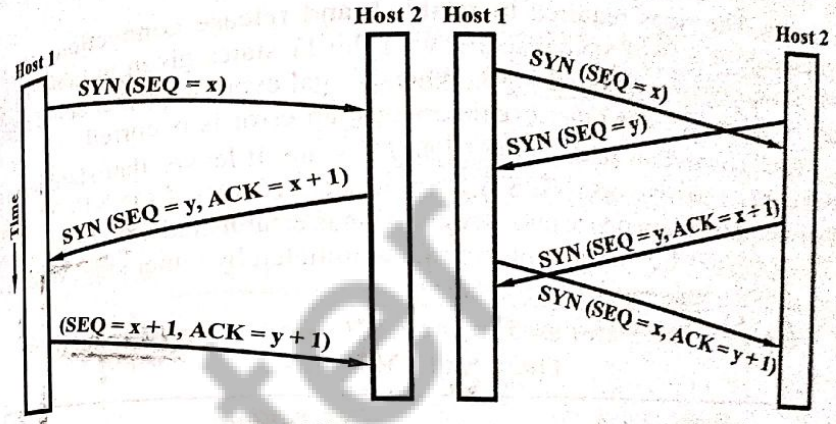
The other side, say, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept and optionally some user data (e.g., a password). The CONNECT primitive sends a TCP segment with the *SYN* bit on and *ACK* bit off and waits for a response.

When this segment arrives at the destination, the TCP entity there checks to see if there is a process that has done a LISTEN on the port given in the ***destination port*** field. Otherwise it sends a reply with the *RST* bit on to reject the connection.

If some process is listening to the port, that process is given the incoming TCP segment. Then, it can either accept or reject the connection. If it accepts, an acknowledgement segment is sent back. Fig. 5.4 (a) shows the sequence of TCP segments sent in the normal case. Note that a *SYN* segment consumes 1 byte of sequence space so that it can be acknowledged unambiguously.

In the event that two hosts simultaneously attempt to establish a connection between the same two sockets. This sequence of events is as shown in fig. 5.4 (b). The result of these events is that just one connection is established, not two because connections are identified by their end points. If the first setup results in a connection identified by (x, y) and the second one does too, only one table entry is made, namely, for (x, y).

A clock-based scheme is used, with a clock tick every 4 μsec. For additional safety, when a host crashes, it may not reboot for the maximum packet lifetime (120 sec) to ensure that no packets from previous connections are still roaming around the Internet somewhere.



(a) TCP Connection Establishment in the Normal Case ***(b) Call Collision***

Fig. 5.4

TCP Connection Release – However, TCP connections are full duplex, to understand how connections are released it is best to think of them as a pair of simplex connections. Each simplex connection is released independently of its sibling. To release a connection, either user can send a TCP segment with the *FIN* bit set, which means that it has no more data to transmit. When the *FIN* is acknowledged, that direction is shut down for new data. However, data may continue to flow indefinitely in the other direction. When both directions have been shut down, the connection is released. Generally, four TCP segments are needed to release a connection, one *FIN* and one *ACK* for each direction. However, it is possible for the first *ACK* and the second *FIN* to be contained in the same segment, reducing the total count to three.

Similar as with telephone calls in which both people say goodbye and hang up the phone simultaneously, both ends of a TCP connection may send *FIN* segments at the same time. These are each acknowledged in the usual way and the connection is shut down. In fact, there is no difference between the two hosts releasing sequentially or simultaneously.

Q.18. Explain the working of TCP protocol and how the connection is released in a TCP. ***(R.G.P.V., Dec. 2014)***

Ans. **TCP Protocol** – Refer the ans. of Q.12.

TCP Connection Release – Refer the ans. of Q.17.

Q.19. How does TCP manage connections in the network ? Discuss thoroughly.

Or

Write short note on finite state machine. ***(R.G.P.V., Dec. 2012)***

Ans. The steps required to establish and release connections can be represented in a finite state machine with the 11 states given in table 5.1. In each state, certain events are legal. When a legal event happens, some action may be taken. If some other event happens, an error is occurred.

Each connection starts in the *CLOSED* state. It leaves that state when it does either a passive open (LISTEN) or an active open (CONNECT). If the other side does the opposite one, a connection is established and state becomes *ESTABLISHED*. Connection release can be initiated by either side. When it is complete the state returns to *CLOSED*.

Table 5.1 The States used in the TCP Connection Management Finite State Machine

State	*Description*
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off

The finite state machine is shown in fig. 5.5. The common case of a client actively connecting to a passive server is shown with heavy lines, solid for the client, dotted for the server. The lightface lines are unusual event sequences. Each line in fig. 5.5 is marked by an ***event/action*** pair. The event can either be a user-initiated system call (CONNECT, LISTEN, SEND, or CLOSE), a segment arrival (*SYN, FIN, ACK,* or *RST*), or, in one case, a timeout of twice the maximum packet lifetime. The action is the sending of a control segment (*SYN, FIN,* or *RST*) or nothing, indicated by comments are shown in parentheses.

One can best understand the diagram by first following the path of a client, then later following the path of a server. When an application program on the client machine issues a CONNECT request, the local TCP entity creates a connection record, marks it as being in the *SYN SENT* state and sends a *SYN* segment. Notice that many connections may be open (or being opened) at the same time on behalf of multiple applications, so the state is per connection and recorded in the connection record. When the *SYN + ACK* arrives. TCP sends the final *ACK* of the three-way handshake and switches into the *ESTABLISHED* state. Now, data can be sent and received.

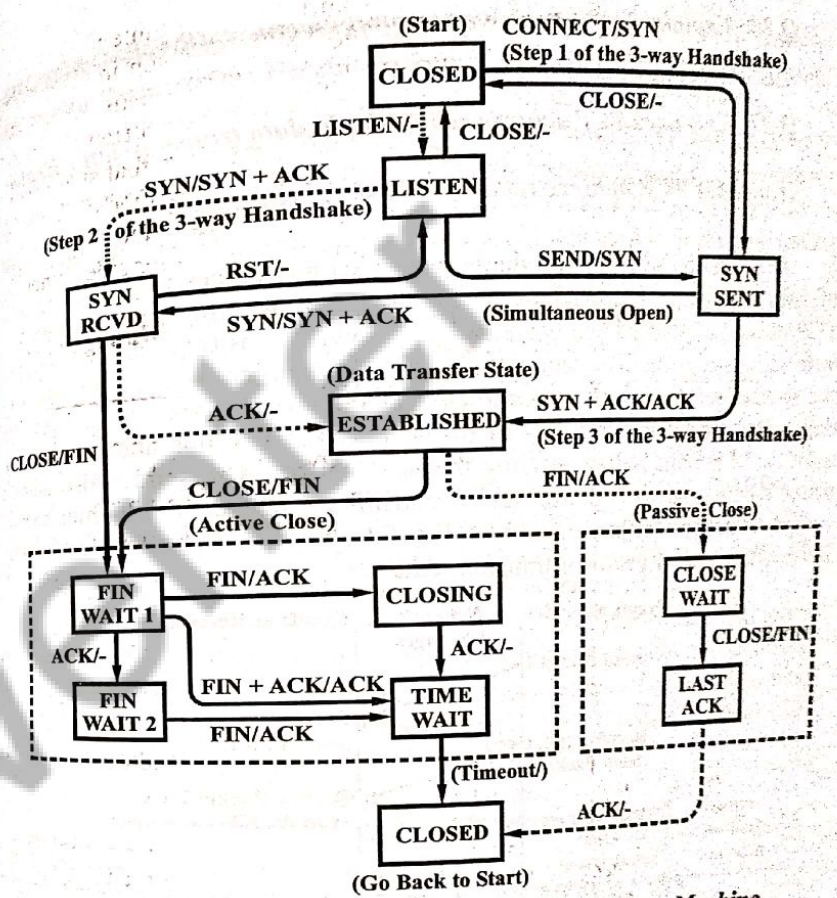


Fig. 5.5 TCP Connection Management Finite State Machine

When an application is finished, it executes a CLOSE primitive, which causes the local TCP entity to send a *FIN* segment and wait for the corresponding *ACK* (dashed box marked active close). When the *ACK* arrives, a transition is made to state *FIN WAIT 2* and one direction of connection is now closed. When the other side closes, too, a *FIN* comes in, which is acknowledged. Now both sides are closed, but TCP waits a time equal to the maximum packet lifetime to guarantee that all packets from the connection have died off. Similarly, in case of acknowledgement was lost. When the timer goes off, TCP deletes the connection record.

Now, let us examine connection management from the server's point of view. The server does a LISTEN and settles down to see who turns up. When a *SYN* comes, it is acknowledged and the server goes to the *SYN RCVD* state. When the server's *SYN* is itself acknowledged, the three-way handshake is complete and the server goes to the *ESTABLISHED* state.

Q.20. Explain TCP connection management. ***(R.G.P.V., May 2019)***

Ans. Refer the ans. of Q.17 and Q.19.

Q.21. How does TCP achieve reliability in data transmission ? Explain.

Or

How does TCP achieve reliability in data transmission ?

(R.G.P.V., June 2017)

Ans. The reliable stream delivery service guarantees to deliver a stream of data sent from one machine to another without duplication or data loss. TCP uses a single fundamental technique known as positive acknowledgement with retransmission. The technique requires a recipient to communicate with the source, sending back an acknowledgement (ACK) message as it receives data. The sender keeps a record of each packet it sends and waits for an acknowledgement before sending the next packet. The sender also starts a timer when it sends a packet and retransmits a packet if the timer expires before an acknowledgement arrives. Fig. 5.6 shows how the simplest positive acknowledgement protocol transfers data.

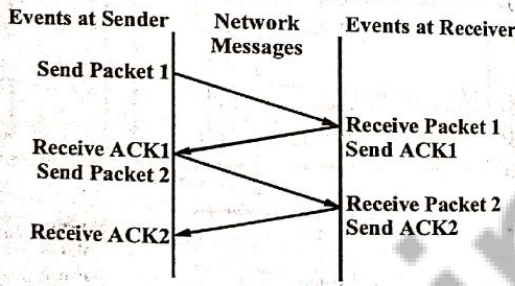


Fig. 5.6 TCP Using Positive Acknowledgement

The final reliability problem aries when an underlying packet delivery system duplicates packets. Duplicates can also arise when networks experience high delays that cause permature retransmission. Solving duplication requires careful though because both packets and acknowledgements can be duplicated. Usually, reliable protocols detect duplicate packets by assigning each packet a sequence number and requiring the receiver to remember which sequence numbers it has received. To avoid confusion caused by delayed or duplicated acknowledgement, positive acknowledgement protocols send sequence numbers back is acknowledgements, so the receiver can correctly associate acknowledgements with packets.

Q.22. How flow control is exercised in TCP/IP ?

Or

Explain flow control in TCP. ***(R.G.P.V., Dec. 2016)***

Ans. Flow control specifies the amount of data a source can send before receiving an acknowledgement from the destination. In a rare case, a transport

layer protocol could send 1 byte of data and wait for an acknowledgement before sending the next byte. But this process is very slow. If the data is traveling along distance, the source is idle while it waits for an acknowledgement.

At the other extreme case, a transport layer can send all of the data it has without worrying about acknowledgement. This speeds up the process, but it may overwhelm the receiver. Moreover, if some part of the data is missed, duplicated, received out of order, or corrupted, the source will not know until all has been checked by the destination.

TCP provides a solution for it. It defines a window that is imposed on the buffer of data delivered from the application program and is ready to be sent. TCP sends as much data as is defined by the sliding window protocol.

Sliding Window Protocol – TCP uses a sliding window protocol to accomplish flow control. In this method, both hosts use a window for each connection. The window spans a portion of the buffer containing bytes that a host can send before worrying about an acknowledgement from the other host. The window is known as the ***sliding window*** as it can slide over the buffer as data and acknowledgements are sent and received.

Fig. 5.7 shows the sender buffer. In fig. 5.7, the bytes before 200 have been sent and acknowledged. Now, the sender can reuse these locations. Bytes 200 to 202 have been sent, but not acknowledged. The sender has to keep these bytes in the buffer because they can be lost or damaged. Bytes 203 to 211 are in the buffer but have not yet been sent.

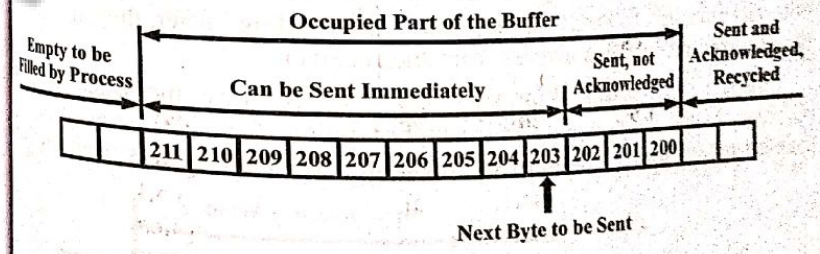


Fig. 5.7 Sender Buffer

Now assume a situation in which there is no sliding window protocol. In this case, the sender can go ahead and send all the bytes (upto 211) in its buffer, without regard to the condition of the receiver. The receiver's buffer, with its limited-size could completely fill up as the receiving process is not consuming data fast enough. The excess bytes thrown away by the receiver will need retransmission. The sender must adjust itself to the number of locations present at the receiver site.

Receiver Window – The receiver buffer is shown in fig. 5.8. Now, the next byte to be consumed by the process is byte 194. The receiver expects to receive byte 200 from the sender. Generally if the total size of the receiving buffer is P and Q locations are already occupied, then only P-Q more bytes

can be received. This value is known as the ***receiver window***. For example, if P = 13 and Q = 6, this specifies that the value of the receiver window is 7.

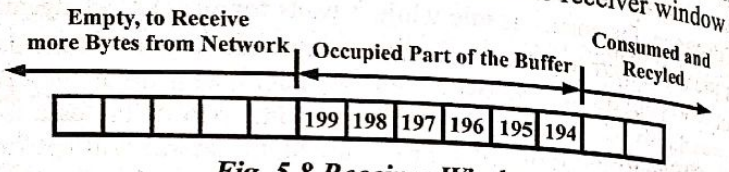


Fig. 5.8 Receiver Window

Sender Window – Flow control can be made if the sender creates a window with a size lower than or equal to the size of the receiver window. This window includes the bytes sent and not acknowledged and those that can be sent. The sender buffer with the sender window is shown in fig. 5.9.

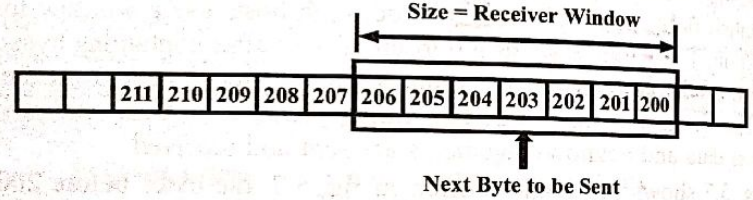
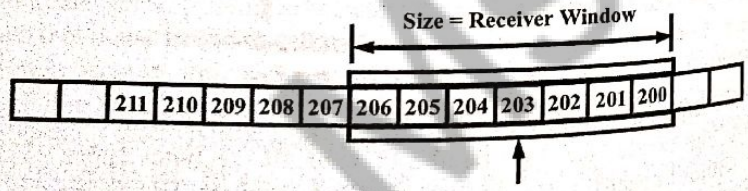


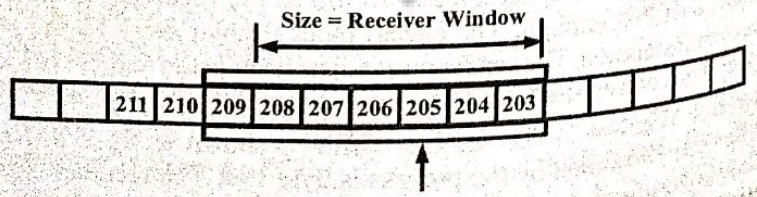
Fig. 5.9 Sender Buffer and Sender Window

Here, notice that the size of the sender window (i.e., 7) is equal to the size of the receiver window. But this does not implies that the sender can send 7 more bytes; it can send only 4 more bytes as it has already sent 3 bytes. Also note that although bytes 207 to 211 are in the sending buffer, they also cannot be sent until more news arrives from the receiver.

Sliding the Sender Window – Here, we see how messages from the receiver change the position of the sender window. Consider, in our example, that the sender sends 2 more bytes and an acknowledgement is received from



(a) Before



(b) After

Fig. 5.10 Sliding the Sender Window

the receiver (expecting byte 204) with no change in the size of the receiver window (still 7). The sender can now slide its window and the locations occupied by bytes 200-202 can be recycled. The position of the sender buffer and the sender window before and after this process (event) is shown in fig. 5.10. In the second part of the figure, the sender can now send bytes 205 to 209 (5 more bytes).

Expanding the Sender Window – The size of the receiver window expands if the receiving process consumes data faster than it receives. This situation increases the window size. In fig. 5.11, the receiver has acknowledged the receipt of 2 more bytes and at the same time has increased the value of the receiver window to 10. In the meantime, the sending process has created 4 more bytes and the sending TCP has sent 5 bytes.

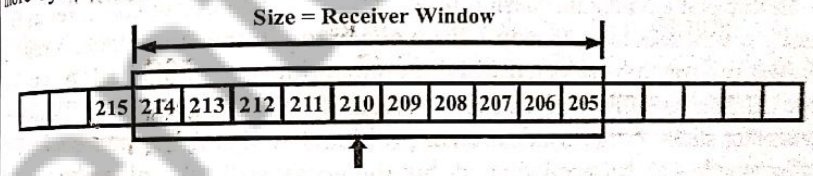


Fig. 5.11 Expanding the Sender Window

Shrinking the Sender Window – The size of the receiver window decreases if the receiving process consumes data slower than it receives. This is the case when the receiver has to inform the sender to shrink its sender window size. In fig. 5.12, the receiver has received the 5 bytes (205 to 209); however, the receiving process has consumed only 1 byte, which implies the number of free locations is reduced to 6 (10 – 5 + 1). It acknowledges bytes 205 to 209 (expecting 210), but also informs the sender to decrease its window size and not to send more than 6 more bytes. If the sender has already sent 2 more bytes when it receives the new and has received 3 more bytes from the sending process, we have the following window and the buffer as shown in fig. 5.12.

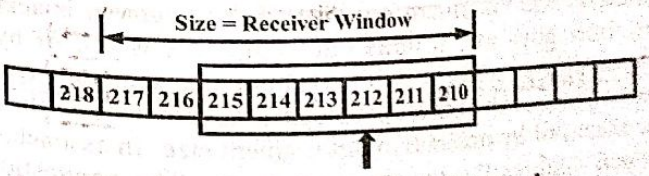


Fig. 5.12 Shrinking the Sender Window

Closing the Sender Window – If the receiver buffer is totally full, then in this case the receiver window value is zero. When this is relayed to the sender, the sender closes its window (left and right walls overlap). The sender cannot send any bytes until the receiver announces a nonzero receiver window value.

Q.23. How congestion control is exercised in TCP ?

Ans. Congestion occurs when the load provided to any network is more than it can handle. Although the network layer attempts to deal with congestion,

most of the heavy lifting is done by TCP as the actual solution to congestion is to slow down the data rate.

Theoretically, congestion is handled by the law of packets conservation. TCP tries to get this goal by dynamically manipulating the window size. The first step in dealing with congestion is detecting it. In the old days, detecting congestion was tremendous task. A timeout occurred due to a lost packet could have been occurred by either noise on a transmission line or packet discard at a congested router. In recent days, packet loss due to transmission errors is usually rare as most long-haul trunks are fibre. As a result, most transmission timeouts on the Internet are due to congestion. Thus, all the Internet TCP algorithms consider that timeouts occurred due to congestion and monitor timeouts for signs of trouble.

Before going on the discussion how TCP reacts to congestion, let us first specify what it does to try to stop it from occurring in the first place. A relative window size has to be selected when a connection is established. A window depending on its buffer size can also be specified by the receiver. When the transmitter sticks to this window size, problems will not happen because of buffer overflow at the receiving end, but they may still take place because of internal congestion within the network.

The Internet solution is to consider that two problems exist – receiver and network capacities – and to monitor each of them individually. To do so, each sender preserves two windows – the window the receiver has granted and a second window, the congestion window. Each indicates the number of bytes the sender may transmit. The number of bytes that may be sent is not the maximum of the two windows. Therefore, the effective window is the minimum of what the sender thinks is all right and what the receiver thinks is all right.

When a connection is established, the congestion window is initialized by the sender to the size of the maximum segment in use on the connection. Then it transmits one maximum segment. If this segment is acknowledged before the timer goes off, it adds one segment's worth of bytes to the congestion window to make it two maximum size segments and transmits two segments. Since each of these segments is acknowledged, the congestion window is enhanced by one maximum segment size. In essence, each burst acknowledged doubles the congestion window. The congestion window enlarges exponentially until either a timeout occurs or the receiver's window is attained. The rationale is that if bursts of size 1024, 2048 and 4096 bytes work fine, but a burst of 8192 bytes causes a timeout, the congestion should be set to 4096 to eliminate congestion. As long as the congestion window is fixed at 4096, no bursts longer than that will be transmitted, no matter how much window space the receiver grants. This algorithm is known as slow start, but it is not slow at all. It is exponential. All TCP implementations are needed to support it.

Q.24. Explain about the various fields of TCP header with the help of neat diagram. ***(R.G.P.V., June 2012)***

Or

Write short note on TCP header format. ***(R.G.P.V., June 2014)***

Ans. The format of the TCP header is shown in fig. 5.13. Its size is varying between 20 to 60 bytes.

(i) Source Port Address – This 16-bit field specifies the port number of the application program in the host that is sending the segment.

(ii) Destination Port Address – This 16-bit field specifies the port number of the application program in the host that is receiving the segment.

(iii) Sequence number – This is a 32-bit field that specifies the number assigned to the first byte of data contained in this segment.

(iv) Acknowledgement Number – This is a 32-bit field that specifies the byte number that the receiver of the segment is expecting to receive from the other party.

(v) Header Length (HLEN) – This is a 4-bit field that tells how many 4-byte words are contained in the TCP header. The header length can be between 20 and 60 bytes. Thus the value of this field will be 5 ($5 \times 4 = 20$) and 15 ($15 \times 4 = 60$).

(vi) Reserved – This 6-bit field is reserved for future use.

(vii) URG – The URG bit is set to 1 to indicate that the value of the urgent pointer field is valid.

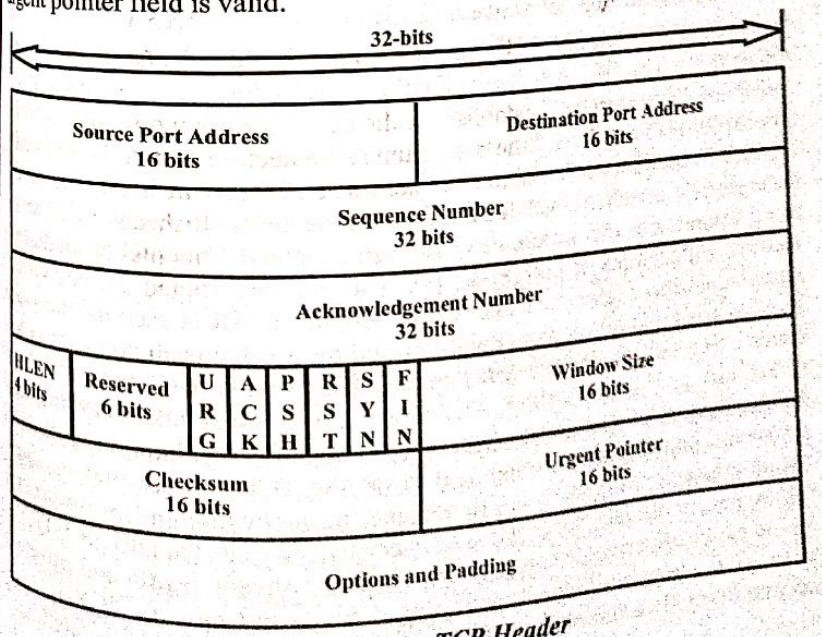


Fig. 5.13 The TCP Header

(viii) ACK – ACK bit is set to 1 if the value of the acknowledgement field is valid.

(ix) PSH – This 1-bit flag specifies PUSHed data.

(x) RST – This 1-bit flag is used to reset a connection that has become confused due to a host crash or some other reason.

(xi) SYN – This 1-bit long flag is used to establish a connection.

(xii) FIN – This 1-bit flag is used to release a connection. It tells that the sender has no more data to transmit.

(xiii) Window Size – This is a 16-bit field that specifies the size of the window, in bytes, that the other party must maintain. The length of this field is 16-bits. It means that the maximum size of the window is 65,535 bytes.

(xiv) Checksum – This 16-bit long field is provided for extra reliability. It checksums.the header, and the data, when performing this computation, the TCP checksum field is set to zero.

(xv) Urgent Pointer – This 16-bit field is valid only if the urgent flag is set. This pointer is used when the segment contains urgent data.

(xvi) Options – This field provides a way to add extra facilities not covered by the regular header. There can be upto 40 bytes of optional information in the TCP header.

Q.25. Briefly explain two protocols used in transport layer for Internet. Explain the TCP service model and segment header. (R.G.P.V., June 2015)

Ans. Refer the ans. of Q.4 and Q.12.

TCP Service Model – TCP service can be found by consisting both the transmitter and receiver generate end points, referred to sockets. Every socket contain a socket number having of the IP address of the host and a 16-bit number local to that host, known as part. A connection should be explicitly established between socket on the transmitting and receiving machines. At the same time, a socket is used for multiple connections. It means that two or more connections can terminate at the same socket. The socket identifiers identify connections at both ends. (i.e. sockets and, socket 2). No virtual circuit numbers or other identifiers can be employed. All TCP connections are point to point and full duplex. Point-to-point means that each connection has exactly two end points and full duplex means that traffic can go in both directions at the same time. TCP does not support broadcasting and multicasting. A TCP connection is a byte stream. Message boundaries are not preserved end-to-end. Another feature of the TCP service that is worth mentioning here is urgent data. The transmitting application puts some control information in the data stream when an interactive user hits the DEL or CTRL-C key to break off a remote computation which has already begun and provides it to TCP along with the urgent flag. This event causes TCP to stop accumulating data and send everything it has for that connection immediately.

The receiving application is interrupted when the urgent data are received at the destination. The end of the urgent data is marked, thus the application knows if it is over. The start of the urgent data is not maked, it is upto the application to figure that out. Basically this technique gives a crude signaling mechanism and leaves everything else up to the application.

TCP Segment Header – Refer the ans. of Q.24.

Q.26. Explain in detail about the TCP timer management.

Ans. Several timers are used by TCP to perform its task. The important one is the retransmission timer. When a segment is transmitted, a retransmission timer is started. The timer is stopped if the segment is acknowledged before the timer expires. On the other hand, when the timer times out before the acknowledgement comes in, the segment is retransmitted. This timer is not the only one which is used by TCP. A second timer known as persistence timer is also employed by the TCP. It is designed to prevent the following deadlock. An acknowledgement with a window size of 0 is transmitted by the receiver, telling the sender to wait. After this, the window is updated by the receiver, but the packet with the update is lost. Now both the sender and the receiver are waiting for each other to do something. The sender sends a probe to the receiver when the persistence timer times out. The window size is given by the response to the probe. If it is still zero, the persistence timer is set again and the cycle repeats. If it is nonzero, data can now be transmitted.

A third timer known as keepalive timer is used by some implementations. When a connection has been efficient for a long time, the keepalive timer can time out to cause one side to recognize if the other side is still there. If it is not successful to respond, the connection is terminated. In turn, this characteristic is controversial as it adds overhead and may terminate a healthy connection due to transient network partition. The last timer employed on each TCP connection is the one used in the TIMED WAIT state while closing. It executes for twice the maximum packet lifetime to ensure that when a connection is closed, all packets created by it have died off.

Q.27. Explain transport layer multiplexing and demultiplexing. (R.G.P.V., May 2019)

Ans. As shown in fig. 5.14, the addressing mechanism permits multiplexing and demultiplexing by the transport layer.

Multiplexing – There can be many processes which require to transmit packets at the transmitter site. At any time, there is only one transport layer protocol. This is many-to-one relationship and needs multiplexing. The messages are accepted by the protocol from various processes, differentiated by their assigned port numbers. The transport layer passes the packet to the network layer after adding the header.

Demultiplexing – At the receiver site, the relationship is one-to-many and needs demultiplexing. The datagram is received by the transport layer from the network layer. The transport layer delivers every message to the suitable process based on the port number, after error checking and dropping of the header.

The multiplexing and demultiplexing is shown in fig. 5.14.

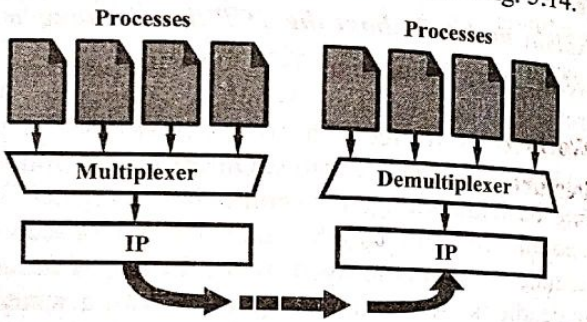


Fig. 5.14

APPLICATION LAYER – WWW AND HTTP, FTP, SSH, EMAIL (SMTP, MIME, IMAP), DNS, NETWORK MANAGEMENT (SNMP)

Q.28. What do you mean by WWW ?

Ans. The world wide web is known as WWW or W3 or Web. The world wide web is an architectural framework for accessing linked documents and repository of information spread all over the Internet. The WWW has a unique combination of flexibility, portability and user-friendly features that distinguish it from other services provided by the Internet. The main reason for its popularity is the use of a concept called ***hypertext.*** Hypertext is a new way of information storage and retrieval, which enables authors to structure information in novel ways. An effectively designed hypertext document can help users to rapidly locate the desired type of information from the vast amount of information on the Internet. Hypertext documents enable this by using a series of links. A link is a special type of item in a hypertext document, which connects the document to another document that provides more information about the linket item.

Hypertext documents on the Internet are known as Web pages. Web pages are created by using a special language called hypertext markup language (HTML). HTML is becoming a de-facto industrial standard for creating Web pages.

The WWW uses the client-server model, and an Internet protocol called hypertext transport protocol (HTTP) for interaction between the computers

on the Internet. Any computer on the Internet, which uses the HTTP protocol is called a ***Web server*** and any computer, which can access that server is called a ***Web client.***

To access a Web page, one requires an address. For any data access distributed all over the world, WWW uses the concept of locators. Any kind of information can be defined on the Internet using the standard URL. URL defines three things – method, host computer and pathname.

Q.29. What is World Wide Web ? Explain the architecture of WWW. ***(R.G.P.V., June 2015)***

Ans. **World Wide Web** – Refer the ans. of Q.28.

Architecture of WWW – The basic model of how the Web works is shown in fig. 5.15. Here, the browser is displaying a Web page on the client machine. When the user clicks on a line of text that is linked to a page on the abcd.com server, the browser follows the hyperlink by sending a message to the abcd.com server asking it for the page. When the page arrives, it is displayed. If this page contains a hyperlink to a page on the xyz.com server that is clicked on, the browser then sends a request to that machine for the page, and so on indefinitely.

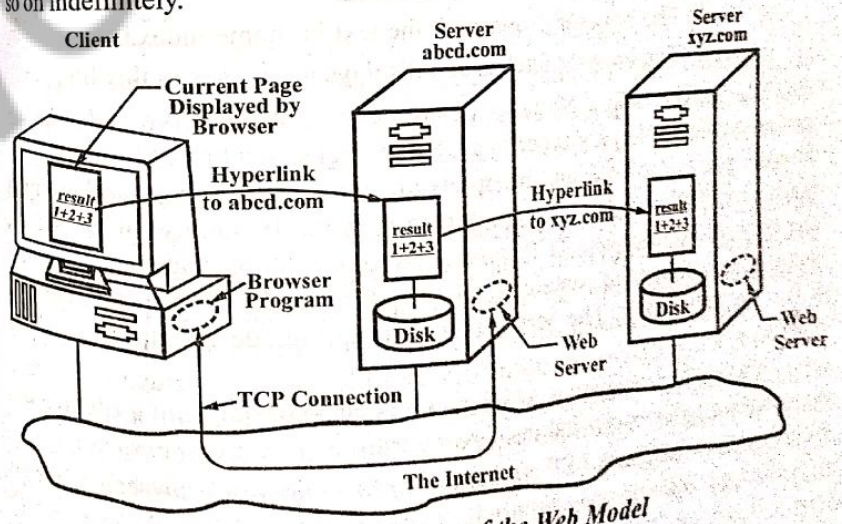


Fig. 5.15 The Parts of the Web Model

The Client Side – Let us now examine the client of fig. 5.15 in more detail. In essence, a browser is a program that can display a Web page and catch mouse clicks to items on the displayed page. When an item is selected, the browser follows the hyperlink and fetches the page selected. Therefore, the embedded hyperlink needs a way to name any other page on the Web Pages are named using URLs (Uniform Resource Locators). A typical URL i

http://www.abcd.com/products.html

For the moment, it is sufficient to know that a URL has three parts –

(i) The name of the protocol (http)

(ii) The DNS name of the machine where the page is located (www.abcd.com)

(iii) The name of the file containing the page (products.html).

If a user click on the hyperlink, the browser carries out a series of steps in order to fetch the page pointed to. Consider a user is browsing the Web and finds a link on Internet telephony that points to ITU's home page, which is http:/www.itu.org/home/index.html. Let us trace the steps that occur when this link is selected.

(i) The browser determines the URL (by seeing what was selected).

(ii) The browser asks DNS for the IP address of www.itu.org.

(iii) DNS replies with 156.106.192.32.

(iv) The browser makes a TCP connection to port 80 on 156.106.192.32.

(v) It then sends over a request asking for file /home/index.html.

(vi) The www.itu.org server sends the file /home/index.html.

(vii) The TCP connection is released.

(viii) The browser displays all the text in /home/index.html.

(ix) The browser fetches and displays all images in this file.

The Server Side – Now, let us take a look at the server side. As we saw above, when the user types in a URL or clicks on a line of hypertext, the browser parses the URL and interprets the part between http://and the next slash as a DNS name to look up. Armed with the IP address of the server, the browser establishes a TCP connection to port 80 on that server. Then it sends over a command containing the rest of the URL, which is the name of a file on that server. The server then returns the file for the browser to display.

To a first approximation, a Web server is given the name of a file to look-up and return. The steps that the server performs in its main loop are –

(i) Accept a TCP connection from a client (a browser).

(ii) Get the name of the file requested.

(iii) Get the file (from disk).

(iv) Return the file to the client.

(v) Release the TCP connection.

Modern Web servers have more features, but in essence, this is what a web server does.

URLs (Uniform Resource Locators) – Web pages may contain pointers to other Web pages. When the Web has first created, it was immediately

apparent that having one page point to another Web page required mechanisms for naming and locating pages. In particular, these questions had to be answered before a selected page could be displayed.

(i) What is the page called ?

(ii) Where is the page location ?

(iii) How can the page be accessed ?

If every page were somehow assigned a unique name, there would not be any ambiguity in identifying pages. Nevertheless, the problem would not be solved.

The solution selected identifies pages in a way that solves all three problems at once. Each page is assigned a URL (Uniform Resource Locator) that effectively serves as the page's worldwide name. URLs have three parts – the protocol (also known as the scheme), the DNS name of the machine on which the page is located, and a local name uniquely indicating the specific page (usually just a file name on the machine where it resides). As an example, the web site for the author's department contains several videos about the using university and the city of Amsterdam. The URL for the video page is

http://www.cs.vu.nl/video/index-en.html.

The URL consists of the three parts – The protocol (*http*), the DNS name of the host (www.cs.vu.nl), and the file name (video/index-en.html), with certain punctuation separating the pieces. The file name is a path relative to the default Web directory at cs.vu.nl.

Cookies – A cookie is information that a website puts on your hard disk so that it can remember something about you at a later time. (More technically it is information for future use that is stored by the server on the client side of a client/server communication). Typically, a cookie, records your preferences when using a particular site. Using the web's hypertext transfer protocol (HTTP) each request for a Web page is independent of all other request. For this reason, the Web page server has no memory of what pages it has sent to a user previously or anything about your previous visits. A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. You can view the cookies that have been stored on your hard disk (although the content stored in each cookie may not make much sense to you). The location of the cookies depends on the browser. Internet explorer stores each cookie as a separate file under a Windows subdirectory. Netscape stores all cookies in a single cookies.txtfile. Opera stores them in a single cookies.dat file.

Cookies are commonly used to rotate the banner ads that a site sends so that it does not keep sending the same ad.

Q.30. Write short note on HTTP. ***(R.G.P.V., June 2014, May 2018)***

Ans. HTTP (Hypertext Transfer Protocol) is the basic underlying application-level protocol used to facilitate the transmission of data to and from a Web server. HTTP provides a simple, fast way to specify the interaction between the client and the server. The protocol actually defines how a client must ask for data from the server and how the server returns it. HTTP does not specify how the data is actually transferred, this is upto lower-level network protocols such as TCP.

HTTP is based on the client/server principle. It allows the client to establish a connection to the server and make a request. The server accepts the connection initiated by the client and sends back a response. HTTP request identifies the resource that the client is interested in and tells the server what action to take on the resource.

Most Web pages are accessed with the Hypertext Transfer Protocol, that is why Web addresses typically begin with http. The http:// at the beginning of a Web page's URL is so common that it often goes without saying. In common usage, the http:// at the beginning of URL often is left out.

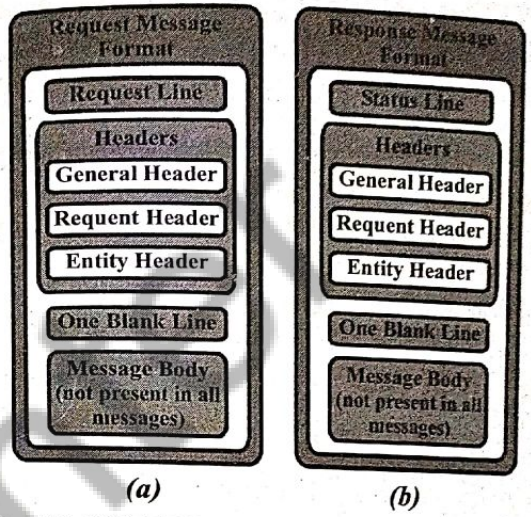
When a user selects a hypertext link, the client program on their computer uses HTTP to contact the server, identifies the resource and asks the server to respond with an action. The server accepts the request and then uses HTTP to respond to or perform the action. Usually, the hypertext links will be blue in colour and will be underlined. When we move the mouse pointer over a hypertext link, the pointer changes its shape to that of a hand. In the case of text based browsers, the hypertext links will be highlighted and we can navigate between them using the keyboard. When we select any of the hypertext links, we are identifying a particular resource and asking the server to send it back to our computer in the format that our computer can display or store.

Hypertext is the text that is specially coded using a standard system called HTML or Hypertext Markup Language. HTML codes are used to create links. These links can be textual or graphic.

Q.31. Write the HTTP request and HTTP response message format. ***(R.G.P.V., May 2019)***

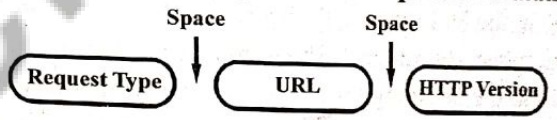
Ans. The HTTP request and response message formats are illustrated in fig. 5.16. A request message is comprised of a request line, a header and sometimes a body as shown in fig. 5.16 (a). The request line consists of request type, URL and HTTP version as shown in fig. 5.17 (a).

A response message is comprised of a status line, a header and sometimes a body as shown in fig. 5.16 (b). The status line consists of HTTP version, status code and status phrase as shown in fig. 5.17 (b).

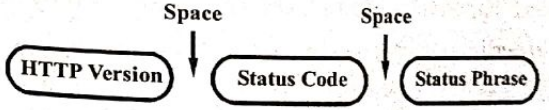


(a) *(b)*

Fig. 5.16 HTTP Request and Response Formats



(a) Request Line



(b) Status Line

Fig. 5.17

The various fields are given below –

(i) Request Line and Status Line – The first line in a request message is called a request line and the first line in the response message is called the status line. There is one common field as shown in fig. 5.17.

(a) Request Type – This field is employed in the request message. HTTP version 1.1 defines various request types which categorize the request message into types of messages known as methods or method tokens. Table 5.2 gives a methods and their functions.

Table 5.2

Methods	*Functions*
PUT	Transmits a document from the server to the client.
HEAD	Requests information about a document but not the document itself.
TRACE	Echoes the incoming request.

GET	Requests a document from the server.
OPTION	Inquires about available options.
POST	Transmits few information from the client to the server.
CONNECT	Reserved.

(b) URL – All Web pages are assigned a unique name to identify them. The name is called URL. It is used for specifying virtually all information on the Internet.

(c) Version – The version field specifies the version of HTTP used. Version 1.1 is the current version of HTTP.

(d) Status Code – In the response message, status code is employed. This field is comprised of three digits. The codes can be described in general terms as follows –

Codes in the 100 range – Informational only
Codes in the 200 range – Show a successful request
Codes in the 300 range – Redirect the client to another URL
Codes in the 400 range – Show an error at the client site
Codes in the 500 range – Show an error at the server site.

(e) Status Phrase – Status phrase field is employed in the response message. The status code in text form is described by the status phrase.

(ii) Header – Header can be used to exchange additional information between the server and the client. HTTP headers can be one or more header lines in which every header line comprises of a header name, a colon, a space and a header value. There are four header categories as given below –

(a) General Header – All HTTP message headers start with the same general header and general header provides general information about the message. General header may be available in both a response and a request.

(b) Request Header – This type of headers are permitted only in request message. Request headers specify the client's configuration and the document format preferred by the client.

(c) Response Header – Response headers are permitted only in response message. Response headers specify the server's configuration and special information about the request.

(d) Entity Header – The information about the body of the document is given by the entity header. Entity headers are sent primarily in response message. Although request messages such as PUT and POST methods can also use entity header.

(iii) Body – It can be present in a request or response message. Generally the body has the document to be transmitted or received.

Q.32. Elaborate the use of FTP. Explain also the FTP process model.

Ans. FTP stands for file transfer protocol. It means that transferring files between computers of different types across the network. A protocol enables computer to communicate to one another. FTP makes files and folders publicly available for transfer over the Internet.

FTP is not designed to enable access to another machine to execute programs, but it is the best utility for file transfer. FTP uses a client-server system in which files are stored at the central computer and transferred between that computer and other widely distributed computers. The central computer runs software called *FTP server* and the software at the other, widely distributed computer runs software called *FTP client.* Using FTP, the client requests that a file transfer be initiated and then the client and server exchange data.

FTP is interactive, a user invokes the FTP application that presents the user with a prompt and waits for the user to enter a command. During interactive session, FTP responds to each command the user enters, and then prints the prompt when it is ready to accept another command. For example, when a session begins, user enters command to identify a remote computer. Then FTP establishes a connection to the remote computer. Similarly, to terminate a session, a user tells FTP to terminate communication with remote computer.

When we log onto the FTP server a connection called a command link is established between the PC and the server. All commands like changing the directory, downloading files, etc., are sent from us to the server via this command link. Now, when the actual downloading process begins a second link called the data link gets established. It is over this data link that the actual download takes place. The connection can open in two modes, i.e., binary and ASCII. In general, we use the binary mode as the file's format does not get changed unlike the ASCII mode. After the file gets downloaded, the data connection closes automatically. It is only when we log out of the FTP that the command link gets broken.

FTP uses two channels. TCP port 20 is the data channel, and port 21 is the command channel. FTP is different from most other TCP/IP application programs in that it does use two channels, enabling simultaneous transfer of FTP commands and data. It also differs in one other important aspect – FTP conducts all file transfers in the foreground, instead of background. In other words, FTP does not use spoolers or queues, so we are watching the transfer process in real time. By using TCP, FTP eliminates the need to worry about reliability or connection management, since FTP can rely on TCP to perform these functions properly.

The basic model of FTP is shown in fig. 5.18. The client has three components the user interface, the client control process, and the client data transfer process. The server has two components the server control process and the server data transfer process. The control connection is made between the control processes. And the data connection is made between the data transfer processes.

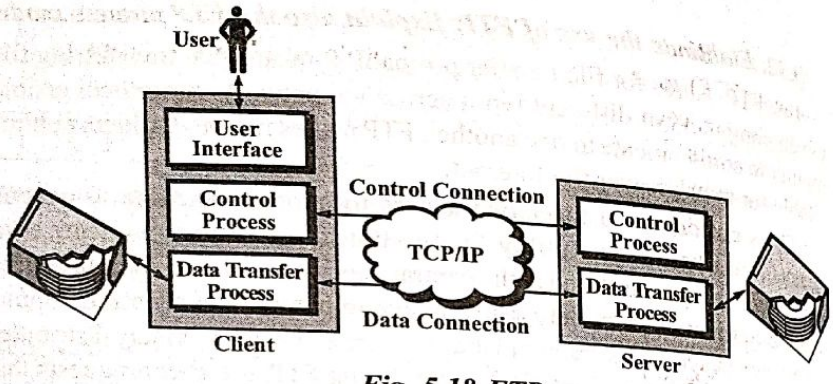


Fig. 5.18 FTP

During the entire interactive FTP session, the control connection remains connected. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. On the other hand, the control connection opens when a user starts an FTP session. The two FTP connections, control and data, use different strategies and different port numbers.

Q.33. Discuss any two protocols of application layer. ***(R.G.P.V., Dec. 2010)***

Ans. Refer the ans. of Q.30 and Q.32.

Q.34. What is FTP ? How FTP differs from other internet-applications and also gives the important features of FTP. ***(R.G.P.V., Dec. 2016)***

Ans. **FTP** – Refer the ans. of Q.32.

FTP differs from other client/server applications in that is setup two connections among the hosts. One connection can be used for control information (commands and responses) and other for data transfer. Dividation of commands and data transfer makes FTP much more efficient. The data connection requires more complex rules because of the variety of data types transferred. On the other hand, the control connection uses very simple rules of communication. At a time, we require to transfer only a command line or a response line. Therefore, the difference in complexity is not TCP at the FTP level. Both control and data connections are treated the same for TCP.

Q.35. What are the various transmission modes of FTP ? ***(R.G.P.V., June 2015)***

Ans. There are three transmission modes of file transfer protocol (FTP) as given below –

(i) Stream Transmission Mode – It is a default mode. Data can be delivered from file transfer protocol (FTP) to transmission control protocol (TCP) as a continuous stream of bytes.

(ii) Block Transmission Mode – Data are delivered from file transfer protocol (FTP) to transmission control protocol (TCP) in terms of blocks. For such case, each block can be proceded by a three byte header. The first byte represents the block descriptor and the next two bytes represent the block size in bytes.

(iii) Compressed Transmission Mode – In this mode, the data are compressed when the file is large. Generally, the run length encoding scheme is used for compression. For this scheme, consecutive data unit appearances may be replaced by one occurrence and the various repetitions.

Q.36. Write short note on SSH. ***(R.G.P.V., June 2016)***

Ans. SSH (Secure Shell) is a point-to-point protocol that is designed to pass encrypted traffic between two specific hosts. Along with tunneling traffic at the presentation layer, SSH also can provide application layer functionality, including a login shell similar to telnet, and FTP-type services. The SFTP system is an implementation of an FTP-like protocol over SSH.

Q.37. What are the phases involved in SSH protocol operations ?

Ans. The SSH protocol operates in the following five phases –

(i) Algorithm Negotiation – SSH supports a variety of cryptographic algorithms. Upon the initial connection, the systems negotiate the cryptographic algorithms that will be used. Different SSH versions and platforms support different algorithms. For encryption, 3DES is required for default compatibility between SSH clients and servers. Other algorithms, such as DES, IDEA, CAST, AES, and Blowfish, are optional. SSH authentication may use RSA or DSA keys. The integrity algorithm depends on the version of SSH. The older version, SSHv1, uses MD5 for performing integrity checks. SSHv2 uses SHA1.

The SSH algorithm negotiation is very similar to SSL. The client offers a list of supported cipher combinations, and the server responds with its selection.

(ii) Key Negotiation – The algorithm negotiation is immediately followed with a key exchange using the Diffie-Hellman (DH) algorithm. SSH performs key exchanges periodically – usually every hour. This way, if an attacker does manage to identify the keys, only a one-hour window of the conversation is compromised. Considering that SSH uses a large key size (512 bits or larger), an attacker is unlikely to crack any session within a usable timeframe.

(iii) Server Authentication – After completing the key exchange, all information is transmitted using encryption. The first data transmitted is the SSH server's public key. If the server has never been seen before, then the client prompts the user to validate the key. After validation, the server's key is

added to the client's list of known servers. However, if the server has been seen before, then the client compares the key with the cached version. If the cache does not match, then the client usually aborts, the SSH user is not prompted to continue when the server fails to validate.

Most SSH clients associate server keys with network addresses. Unfortunately, servers are occasionally reinstalled or assigned new addresses. The result is a mismatch between the server's key and the client's cache. The user must resolve the issue, and the resolution varies with different SSH clients –

(a) OpenSSH – The OpenSSH client is used on most Unix systems. For OpenSSH, users must manually edit their host-key cache files to remove the mismatched server entry. The file is stored in the user's home directory – $HOME/.ssh/known_hosts. For users who connect to many SSH servers, this can be a very large file. To resolve mismatched cache entries, users must edit the file and delete the line for the offending server. This is significantly different from HTTPS, where most browsers prompt users to continue.

(b) PuTTY – For Windows SSH clients, PuTTY is common. PuTTY stores the host-key cache in the Registry under HKEY_CURRENT_USER\Software\SimonTatham\PuTTY. But rather than editing the Registry, PuTTY prompts the user when the host key does not match. The user has the option to accept the new host key and overwrite the old one.

(c) Mocha Telnet – For PocketPC, WindowsCE, PalmOS, mobile phones, and most other platforms, Mocha Telnet is available for supporting SSH. Unlike OpenSSH and PuTTY, Mocha Telnet does not cache server keys. As a result, all servers are always accepted.

Other SSH clients, like F-Secure SSH, ZOC, and Pragma SSH all use different caching methods. Resolving mismatched keys requires knowing the specific type of SSH client.

(iv) Client Authentication – After authenticating the server, the client is authenticated. The client may transmit any combination of a password, a challenge signed by the client key, or a digital identifier for authentication. If the authentication works, then the client successfully connects. If the authentication fails, however, the client is disconnected. SSH servers may permit multiple password retries, but repeated failures result in a disconnection.

(v) Data Transfer – After negotiating the algorithms, exchanging keys, and authenticating both the client and server, an encrypted VPN tunnel is established. The SSH VPN permits multiple channels. Through concurrent channels, SSH supports many simultaneous connections. For example, a login shell may be on channel #0, an X11 graphical traffic on channel #1, and a VPN

proxy on channel #2. All of this data transfers across an encrypted tunnel that changes keys every few minutes.

Q.38. What is an electronic mail ? Explain the basic functions of electronic mail.

Ans. Electronic mail (e-mail) is a process of sending data from one computer to another. This is also called offline service. The message (data) takes anywhere from a few seconds to several minutes to reach its destination, because it must be passed from one network to another, until it reaches its destination. It provides various facilities –

(i) Speedy data transfer (ii) Bulk data transfer in low cost
(iii) Better acknowledgement (iv) Structured data
(v) Simplicity in making carbon copies
(vi) Integrated message, like combination of audio, video, text, graphics.

The e-mail proposals were initially published by ARPANET in 1982. These proposals were called RFC (request for comment) 821 and RFC 822. The FC 821 defines message format. The CCITT defined X.400 standard for e-mail.

Services of E-mail – The e-mail system consists of two parts –

(i) User Agent – It allows people to read and send e-mail.

(ii) Message Transfer Agent – It moves the messages from the source to the destination. The message transfer agents run in the background while the user agents run in the front.

E-mail system supports five basic functions –

(i) Composition – It refers to the process of creating messages and acknowledgements. While answering the mail, the e-mail system abstracts the originator's address and subject field to make a reply.

(ii) Transfer – It refers to the process of moving message from source to destination. It is responsible for establishing connections to the destination of some intermediate machine, outputting the message and releasing the connection.

(iii) Reporting – It is responsible for making replies or acknowledgements. It permits to make a variety of acknowledgements.

(iv) Displaying – It displays the incoming mail in proper format. It also transforms the message if required.

(v) Disposition – It is the final step of e-mail. It is concerned with what the recipient does with the message after receiving it. There are various possibilities – discard, save, forward, etc.

Q.39. Explain SMTP protocol in detail. ***(R.G.P.V., Dec. 2016)***

Or

Write short note on SMTP. ***(R.G.P.V., June 2011, 2012, May 2018)***

Or

Describe working of SMTP protocol in brief. ***(R.G.P.V., Dec. 2015)***

Ans. One of the most common use of networks is electronic mail, the ability to send a message or file to a specific user at a local or remote site. Typically, you send a message by specifying the email address of the recipient. The usual address format is name @host-text-address. The message is buffered at the destination site and is accessible only by the intended user.

In addition to message formats, the TCP/IP protocol suite specifies a standard for the exchange of mail between machines. That is, the standard specifies the exact format of messages a client on the machine uses to transfer mail to a server on another. The standard transfer protocol is known as ***simple mail transfer protocol.*** The SMTP protocol focuses specifically on how the underlying mail delivery system passes messages across an Internet from one machine to another. It does not specify how the mail system accepts mail from a user interface presents the user with incoming mail.

SMTP does not specify how mail is stored or how frequently the mail system attempts to send messages.

Fig. 5.19 shows the interaction between local mail, SMTP, and TCP. When a user sends mail, the local mail facility determines whether the address is local or requires a connection to a remote site. In the latter case, the local mail facility stores the mail, where it waits for the client SMTP. When the client SMTP delivers the mail, it first calls TCP to establish a connection with the remote site. When the connection is made, the client and server SMTPs exchange packets and eventually deliver the mail. At the remote end, the local mail facility gets the mail and delivers it to the intended recipient.

Fig. 5.19 SMTP Interacting with Local Mail and TCP

There are four parameters in SMTP protocol.

(i) Sending Mail – To send mail the user through the UA (User Agent), creates mail that looks very similar to postal mail. It has an ***envelope*** and a ***message.***

(ii) Envelope – The envelope generally contains the sender address, the receiver address, and other information.

(iii) Message – The message contains the ***headers*** and the ***body.*** The headers define the sender, the receiver, the subject of the message, and some other information. The body contains the actual information to be read by the recipient.

(iv) Receiving Mail – The user agent periodically checks the mailboxes. If a user has mail, the UA informs the user first by giving a notice. If the user is ready to read the mail, a list is displayed in which each line contains a summary of information about a particular message in the mailbox.

Q.40. What is the role of SMTP and POP 3 in a mail services ? ***(R.G.P.V., June 2016)***

Ans. SMTP is used to transfers the email message from the SMTP server of the sender to the SMTP server of the recipient. The main function of SMTP is to carry the email message between the sender and the recipient. POP is used for retrieving emails from a remote server for a mail recipient. In other words, any user who wants to receive emails but does not have a permanent connection to the Internet uses a POP client to pull emails from a POP server.

All emails are stored on a centralized email server called SMTP server. The SMTP server expects the destination host to be online all the time. Without this it cannot create a TCP connection with it, and therefore, cannot forward the email message to the destination host. Thus, POP is introduced to resolve such problem. SMTP server receives and stores all the incoming emails for any user and forwards the incoming emails to the user's mailbox. When a user's POP client connects to the POP server, the POP server opens the mailbox for that user and sends the new emails to that user. The current version of POP is 3, and therefore, it is sometimes also called as POP 3.

Q.41. What do you mean by MIME ? Explain its headers.

Ans. MIME (Multipurpose Internet Mail Extensions) is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP and RFC 822 for electronic mail. Some limitations of the SMTP as – SMTP can send messages only in NVT 7-bit ASCII format. It cannot be used for languages that are not supported by 7-bit ASCII characters (such as French, Germen, Hebrew, Russian, Chinese and Japanese). Also, it cannot be used to send binary files or to send video or audio data.

Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol which permits non-ASCII data to be sent through SMTP. MIME is not a mail protocol and cannot replace SMTP; it is only an extension to SMTP.

MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client SMTP to be sent through the Internet. The server SMTP at the receiving side receivers the NVT ASCII data and delivers it to MIME to be transformed back to the original data. MIME is shown in fig. 5.20.

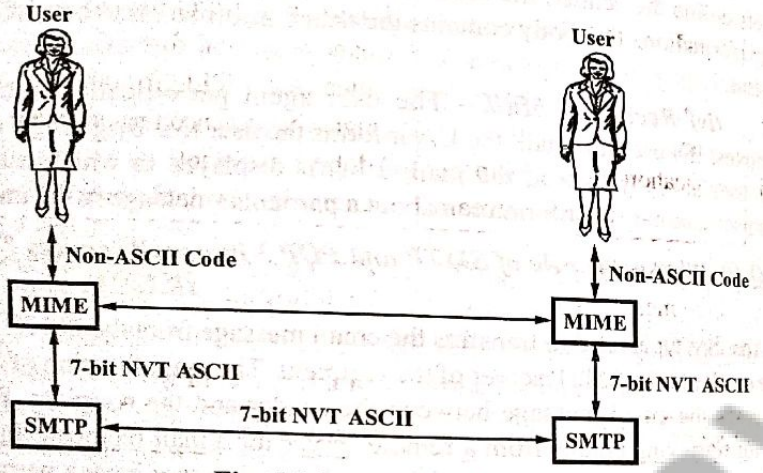


Fig. 5.20 MIME

MIME defines five headers that can be added to the original SMTP header. MIME headers are as follows –

(i) MIME-version – This header defines the version of MIME used. The current version is 1.1. This field indicates that the message conforms to RFC 1521 and 1522.

(ii) Content-type – This header defines the type of data used in the body of the message. The content type and the content subtype are separated by a slash. Depending on the subtype, the header may contain other parameters.

content-Type : <type/subtype; parameters>

MIME allows seven different types of data. These are listed in table 5.3.

Table 5.3 Datatype and Subtype in MIME

S.No.	Type	Subtype	Description
(i)	Text	Plain	Unformatted text
		Mixed	Body contains ordered parts of different data types
(ii)	Multipart	Parallel	Same as above, but no order
		Digest	Similar to Mixed sub types, but the default is message/RFC822
		Alternative	Parts are different versions of the same message
		RFC822	Body is an encapsulated message
(iii)	Message	Partial	Body is a fragment of a bigger message
		External-body	Body is a reference to another message
(iv)	Image	JPEG	Image is in JPEG format
		GIF	Image is in GIF format
(v)	Video	MPEG	Video is in MPEG format
(vi)	Audio	Basic	Single channel encoding of voice at 8 kHz
(vii)	Application	PostScript	Adobe PostScript
		Octet-stream	General binary data (eight-bit bytes)

(iii) Content-transfer-encoding – This header defines the method to encode the messages into 0s and 1s for transport.

The five types of encoding are listed in table 5.4.

Table 5.4 Content-transfer-encoding

Type	Description
7-bit	NVT ASCII characters and short lines
8-bit	Non-ASCII characters and short lines
Binary	Non-ASCII characters with unlimited-length lines
Base 64	6-bit blocks of data are encoded into 8-bit ASCII characters
Quoted-printable	Non-ASCII characters are encoded as an equal sign followed by an ASCII code

(a) 7-bit – This is 7-bit NVT ASCII encoding. Although no special transformation is needed, the length of the line should not exceed 1,000 characters.

(b) 8-bit – This is 8-bit encoding. Non-ASCII characters can be sent, but the length of the line still should not exceed 1,000 characters. MIME does not do any encoding here; the underlying SMTP protocol must be able to transfer 8-bit non-ASCII characters. It is, therefore not recommended.

(c) Binary – This is 8-bit encoding. Non-ASCII characters can be sent and the length of the line can exceed 1,000 characters. MIME does not do any encoding here; the underlying SMTP protocol must be able to transfer binary data.

MSInverter

(d) Base 64 – This is a solution for sending data made of bytes when the highest bit is not necessarily zero. Base 64 transforms this type of data to printable characters, which can then be sent as ASCII characters or any type of character set supported by the underlying mail transfer mechanism. Base 64 divides the binary data into 24-bit blocks.

(e) Quoted–printable – Base 64 is a redundant encoding scheme, that is, 24 bits becomes four characters, and eventually sent as 32 bits. If the data consist of mostly ASCII characters with a small non-ASCII proton. We can use quoted-printable encoding. If a character is ASCII, it is sent as is. If a character is not ASCII, it is sent as three characters. The first character is the equal sign (=). The next two characters are the hexadecimal representation of the byte.

(iv) Content-Id – This header uniquely identifies the whole message in a multiple message environment.

(v) Content-description – This header defines whether the body is image, audio or video.

Q.42. Write short note on Internet Message Access Protocol version 4 (IMAP-4).

Ans. Version 4 of the Internet Mail Access Protocol (IMAP4) is an alternative to POP3. IMAP4 is similar to POP3, but it has more features. IMAP4 is more powerful and more complex.

Like POP3, IMAP4 defines an abstraction known as a mailbox. Mailboxes are located on the same computer as a server. Also like POP3, a user runs an IMAP4 client that contacts the server to retrieve messages. Unlike POP3, however, IMAP4 allows a user to dynamically create, delete, or rename mailboxes.

IMAP4 also provides extended functionality for message retrieval and processing. A user can obtain information about a message or examine header fields without retrieving the entire message. In addition, a user can search for a specified string and retrieve specified portions of a message. Partial retrieval is especially useful for slow-speed dialup connections because it means a user does not need to download useless information.

Q.43. Write short note on DNS in the Internet. ***(R.G.P.V., June 2010)***

Or

Write short note on DNS. ***(R.G.P.V., June 2011, 2013, 2014)***

Or

What is the utility of DNS ? ***(R.G.P.V., June 2015)***

Ans. The essence of DNS is the invention of a hierarchical, domain-based naming scheme and a distributed database system for implementing

he naming scheme. The primary use of DNS is for mapping host names nd e-mail destinations to IP addresses but can also be used for other urposes.

The DNS is a distributed database. It is used by TCP/IP application. We se the term distributed because no single site on the Internet knows all the nformation. Each site maintains its own database of information and runs a erver program that other system across the Internet (clients) can query. The NS provides the protocols that allow client and server to communicate with ach other.

On Unix hosts the resolver is accessed primarily through two library unctions, gethostbyname(3) and gethostbyaddr(3), which are linked with he application when the application is built. The first takes a hostname nd returns an IP address, and the second takes an IP and looks up a ostname. The resolver contacts one or more name servers to do the napping.

The resolver is normally the part of the application. It is not part of the perating system kernel as are the TCP/IP protocols.

RFC 1034 specifies the concept and facilities provided by DNS, and RFC 035 details the implementations and specification.

Q.44. DNS uses UDP instead of TCP. If a DNS packet is lost, there is o automatic recovery. Does this cause a problem ? And if so, how is it olved ? ***(R.G.P.V., June 2016)***

Ans. If a DNS packet is lost or a DNS server is unable to respond, then t can cause problems with applications. DNS is used to handle the resolution f host names to IP addresses. Without this information, an application cannot nitiate a connection with the appropriate host on the network or Internet. For xample, if you type www.yahoo.com into your browser then DNS resolves he address to 66.94.230.38 and the browser try to connect this IP address sing HTTP. When there is a problem with DNS, you see the browser wait for response or it will come back and tell you that it could not find a particular omain. If a DNS packet using UDP is lost this problem must be handled at he application layer.

There are some ways to solve the DNS problem. First is to configure our computer to use multiple DNS servers. In this case, if the primary DNS erver fails, the backup servers will be used to try to resolve the data. A econd, but not very graceful, way around this with critical applications is to ot use hostnames at all, but to use the fixed IP address in the configuration. his circumvents the DNS process completely. DNS is idemportent. Operation an be repeated without harm. When a process makes a DNS request, it starts timer. If the timer expires, it just makes the request again.

Q.45. Explain the services provided by DNS. ***(R.G.P.V., May 2019)***

Ans. There are several services provided by DNS –

(i) Host Aliasing – A host with a complicated hostname can have one or more alias names. For example, a hostname such as relay1.west-coast.enterprise.com could have, say, two aliases such as enterprise.com and www.enterprise.com. In this case, the hostname relay1.west-coast.enterprise.com is said to be ***canonical hostname***. Alias hostnames, when present, are typically more mnemonic than canonical hostnames. DNS can be invoked by an application to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host.

(ii) Mail Server Aliasing – DNS can be invoked by a mail application to obtain the hostname for a supplied alias hostname as well as the IP address of the host. In fact, the MX record permits a company's mail server and web server to have identical (aliased) hostnames; for example, a company's web server and mail server can both be called enterprise.com.

(iii) Load Distribution – DNS is also used to perform load distribution among replicated servers, such as replicated web servers. Busy sites, such as cnn.com, are replicated over multiple servers, with each running on a different end system and having a different IP address. For replicated web servers, a set of IP addresses is thus associated with one canonical hostname. The DNS database contains this set of IP addresses. When clients make a DNS query for a name mapped to a set of addresses, the server responds with the entire set of IP addresses, by rotates the ordering of the addresses within each reply. Because a client typically sends its HTTP request message to the IP address that is listed first in the set, DNS rotation distributes the traffic among the replicated servers.

DNA rotation is also used for e-mail so that multiple mail servers can have the same alias name. Also, content distribution companies such as Akamai have used DNS in more sophisticated ways to provide web content distribution.

Q.46. Explain the concept of SNMP.

Or

Write short note on network management. ***(R.G.P.V., June 2014)***

Ans. Simple network management protocol (SNMP) is a simple tool for network management. As networks grow larger, they become harder to manage. For this reason, SNMP has been devised. It provides a systematic way of monitoring and managing a computer network.

The simplicity is the strength of SNMP. It defines a limited, easily implemented management information base (MIB) of scalar variables and two dimensional tables. This protocol allows managers to communicate with agents inside devices to read out their status and issue commands to them.

SNMP is designed to operate in both the TCP/IP and OSI environment. It is widely implemented in commercial products.

SNMP has some shortcomings that include functional defficiencies and lack of security facility. Due to this, enhanced versions of SNMP; SNMPv2 and SNMPv3 are defined. SNMPv2 contains a number of functional enhancements and provides good security features. SNMPv3 provides authentication, privacy and access control.

The SNMP model of a managed network consists of four components –

(i) Managed nodes (ii) Management stations

(iii) Management information (iv) A management protocol.

The model is illustrated in fig. 5.21 and discussed below –

The managed nodes are the hosts, routers, bridges, printers or any other devices capable of communicating status information to the outer world. To be managed directly by SNMP, a node must be capable of running an SNMP management process, called an ***SNMP agent.*** Each agent maintains a local database of variables that describe its state and history and affect its operation.

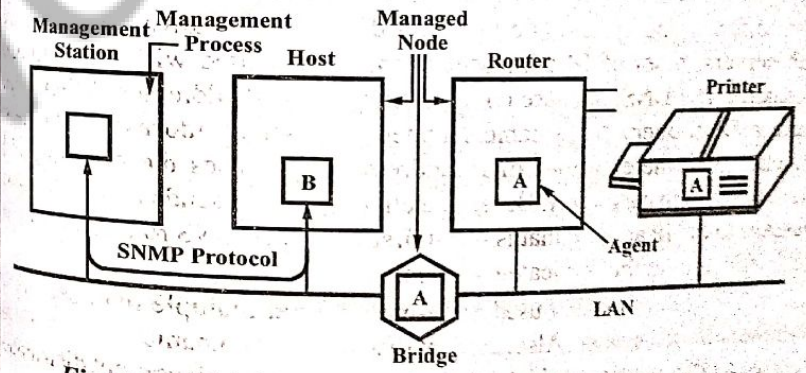


Fig. 5.21 Components of the SNMP Management Model

Network management is done from management stations. These are in fact general-purpose computers that communicate with the agents over the network, issuing commands and getting responses. Management stations bear all the intelligence in the network.

The largest portion of the SNMP model is the management information that contains the definition of whom has to keep track of what and how this information is communicated. Each device maintains one or more objects (variables) that describe its state. The collection of all possible objects in a network is given in a data structure called the MIB (management information base).

The SNMP protocol is used interact the management station with the agents. This management protocol allows the management station to query the state of an agent's local objects and change them if necessary. Most of SNMP consists of this query response type communication.

■■■

RGPV

B.E. (Sixth Semester) EXAMINATION, June 2011
(Computer Science & Engg. Branch)
COMPUTER NETWORKING
[CS–604(N)]

Note : Attempt *one* question from each Unit. All questions carry equal marks.

Unit-I

1. (a) Write difference between OSI and TCP/IP model. 10

(See Unit-I, Page 36, Q.36)

(b) Define three layers of X.25. ** 10

Or

2. (a) Write a short note on TCP & UDP. 10

(See Unit-V, Page 189, 184, Q.12, Q.4)

(b) Compare ATM and Frame relay. ** 10

Unit-II

3. (a) Given an error free 64 kbps satellite channel which is used to send 512 byte data frames in one direction with very short acknowledgements coming back the other way. What will be the maximum throughput for window size of 1, 7, 15 and 127 ? 15

(See Unit-II, Page 86, Prob.3)

(b) State various design issues for Data link layer. 5

(See Unit-II, Page 56, Q.2)

Or

4. (a) What is meant by bit stuffing ? Explain. (See Unit-II, Page 60, Q.5) 10

(b) Draw and explain about the frame structure and various frame types in HDLC. ** 10

Unit-III

5. (a) What is need of minimum frame size ? (See Unit-III, Page 114, Q.28)
If it is 64 byte, then calculate loss of bandwidth for 100 mbps Ethernet network ? 14

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Msinventer

(b) Define FDDI.

Or ** 6

6. (a) How can you compare 1-persistent CSMA and P-persistent CSMA ? (See Unit-III, Page 111, Q.22) 10

(b) Explain the MAC frame format. (See Unit-III, Page 132, Q.46) 10

Unit-IV

7. (a) How many host per network in each IP address class can exist ? Show with example. (See Unit-IV, Page 168, Q.30) 8

(b) Define the types of Routing algorithms. (See Unit-IV, Page 146, Q.8) 12

Or

8. (a) How can you compare IPv4 and IPv6 ? 10 (See Unit-IV, Page 181, Q.47)

(b) What are unicast routing protocols ? (See Unit-IV, Page 148, Q.12) 10

Unit-V

9. (a) How would you define congestion control and QoS ? ** 10

(b) What is the difference between IP addresses and port number ? ** 10

Or

10. Write short notes on the following – 5 each

(i) Virtual terminal protocol **

(ii) H.323 layering **

(iii) SMTP (See Unit-V, Page 216, Q.39)

(iv) DNS. (See Unit-V, Page 220, Q.43)

RGPV

B.E. (Sixth Semester) EXAMINATION, June 2012
(Computer Science Engg. Branch)
COMPUTER NETWORKING
(CS-604)

Note : Attempt *one* question from each Unit. All questions carry equal marks.

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Unit-I

1. (a) What are the components of Computer Network ? Explain goals o Computer Network. (See Unit-I, Page 7, Q.5) 10

(b) A 100 km long cable runs at T_1 data rate. The propagation speed in the cable is 200000 km/sec. How many bits fit in the cable ? 4

**

(c) Describe the design issues for the layers. (See Unit-I, Page 25, Q.24) 6

Or

2. (a) What are the various network topologies ? List the factors that affect the choice of a topology and transmission medium in a LAN. 10 (See Unit-I, Page 11, Q.8)

(b) Explain connection oriented and connectionless services with examples. (See Unit-I, Page 21, Q.21) 6

(c) What is the difference between Internet, Intranet and Extranet ? ** 4

Unit-II

3. (a) Given an error free 64 kbps satellite channel which is used to send 512 byte data frame in one direction with very short acknowledgements coming back the other way. What will be the maximum throughput for window size 1, 7, 15 and 127 ? 10 (See Unit-II, Page 86, Prob.3)

(b) What are various framing methods ? Explain. 6 (See Unit-II, Page 57, Q.3)

(c) What is Piggybacking ? (See Unit-II, Page 64, Q.14) 4

Or

4. (a) A channel has a bit rate of 4 kbps and propagation delay of 20 msec. For what range of frame size does stop and wait protocol give a efficiency of at least 50% ? (See Unit-II, Page 85, Prob.1) 8

(b) Explain sliding window protocol. (See Unit-II, Page 68, Q.20) 8

(c) Compare bridges and layer-2 switches. ** 4

Unit-III

5. (a) Explain slotted ALOHA protocol. Derive efficiency for slotted ALOHA protocol. (See Unit-III, Page 107, Q.18) 10

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Msinventer

(b) What do you mean by limited contention protocol ? Explain any *one*. 10

(See Unit-III, Page 125, Q.35)

Or

6. (a) A large population of ALOHA users manages to generate 50 request/sec, including both originals and retransmissions. Time is slotted in unit of 40 msec – 10

(i) What is the chance of success on the first attempt ?

(ii) What is the probability of exactly k collisions and then a success ?

(iii) What is expected number of transmission attempts needed ?

(iv) What is throughput of channel ?

(See Unit-III, Page 118, Prob.3)

(b) Differentiate between 802.3, 802.4 and 802.5 IEEE standard. 10

(See Unit-III, Page 136, Q.53)

Unit-IV

7. (a) A host in an organization has an IP address 150.37.64.34 and a subnet mask 255.255.240.0. What is the address of this subnet ? What are the ranges of IP address that is host can have on this subnet ? 10

(See Unit-IV, Page 182, Prob.3)

(b) What are the limitations of IPv4 ? Compare IPv4 and IPv6. 10

(See Unit-IV, Page 182, Q.43)

Or

8. (a) What do you mean by Congestion in Subnet ? Explain congestion control in datagram subnet. ** 10

(b) What do you mean by Routing ? What are various types of routing algorithms ? Explain any *one*. 10

(See Unit-IV, Page 146, Q.9)

Unit-V

9. (a) Explain about the various fields of TCP header with the help of neat diagram. 10

(See Unit-V, Page 201, Q.24)

(b) What is UDP ? In case where reliability is not a primary importance, UDP would make a good transport protocol. Give example of specific case. 10

(See Unit-V, Page 185, Q.5)

Or

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

10. Write short notes on the following – 5 each

(a) Digital signature **

(b) Virtual terminal protocol **

(c) SMTP (See Unit-V, Page 216, Q.39)

(d) VoIP. **

RGPV

B.E. (Sixth Semester) EXAMINATION, Dec. 2012
COMPUTER NETWORKING
(CS-604)

Note : Attempt one question from each unit.
All questions carry equal marks.

Unit-I

1. (a) What is the principal difference between connectionless communication and connection oriented communication ? 10

(See Unit-I, Page 21, Q.21)

(b) Consider 2^n-1 MPs connected by the following topologies –

(a) Star

(b) Ring

(c) Complete interconnection

for each give the no. of hoPs needed for the average IMP-IMP Packet. 10

Or

2. (a) Explain the OSI Model in detail. (See Unit-I, Page 27, Q.27) 10

(b) What is computer network and how it is different from distributed system ? (See Unit-I, Page 3, Q.2) 10

Unit-II

3. (a) Explain Go-back-N Protocol in detail. (See Unit-II, Page 82, Q.30) 10

(b) A channel has bit rate of 4 Kbps and propagation delay of 20 msec. For what range of frame size does stop and wait give an efficiency of at least 50%. (See Unit-II, Page 85, Prob.1) 10

Or

4. (a) Write short note on high level data link control protocol. 10 **

(b) Explain 1 bit sliding window protocol. (See Unit-II, Page 72, Q.24) 10

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

MSInverter

Unit-III

5. (a) What is the difference between slotted ALOHA and Pure ALOHA ? (See Unit-III, Page 105, Q.13) 10

(b) How does CSMA/CD differ from CSMA/CA ? (See Unit-III, Page 117, Q.32) 10

Or

6. (a) Compare a piconet and Scatternet. (See Unit-III, Page 142, Q.56)

(b) Write short note on FDDI Protocol. ** 10

Unit-IV

7. (a) What is the difference between unicast routing and Multicast routing ? (See Unit-IV, Page 162, Q.24) 10

(b) Write the difference between IPv4 and IPv6. (See Unit-IV, Page 181, Q.47) 10

Or

8. (a) Explain Dijkstra algorithm with example. (See Unit-IV, Page 150, Q.13) 10

(b) Differentiate between congestion control and flow control. ** 10

Unit-V

9. (a) Explain the main features of transmission control protocol. (See Unit-V, Page 191, Q.14) 10

(b) What is network security and write the aspects of network security ? ** 10

Or

10. Write short note (any 2) – 20

(a) Digital signature **

(b) ATM **

(c) Cryptography **

(d) Finite state machine. (See Unit-V, Page 193, Q.19)

RGPV

B.E. (Sixth Semester) EXAMINATION, June 2013
(Computer Science Engg. Branch)
COMPUTER NETWORKING
(CS-604)

Note : Attempt *one* question from each Unit. All questions carry equal marks.

Unit-I

1. (a) What is computer Network ? Write advantages of computer Network. (See Unit-I, Page 3, Q.1) 10

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

(b) What are the reasons of using layered protocol ? (See Unit-I, Page 18, Q.16) 10

Or

2. (a) Explain in detail TCP/IP reference model. (See Unit-I, Page 33, Q.33) 10

(b) Explain the difference between a virtual channel connection (VCC) and a virtual path connection (VPC). ** 10

Unit-II

3. (a) Describe the working of a selective repeat protocol. (See Unit-II, Page 82, Q.30) 10

(b) Explain the finite state machine model for protocol verification. (See Unit-II, Page 87, Q.35) 10

Or

4. (a) What is bit stuffing ? If the bit string 0111101111101111110 is subjected to bit stuffing. What is the output string ? (See Unit-II, Page 61, Q.6) 10

(b) Explain sliding window protocol in detail. (See Unit-II, Page 68, Q.20) 10

Unit-III

5. (a) Explain why the efficiency of pure ALOHA is half of slotted ALOHA. (See Unit-III, Page 106, Q.15) 10

(b) Explain CSMA protocol in detail. (See Unit-III, Page 108, Q.19) 10

Or

6. (a) Explain FDDI in detail. ** 10

(b) Ten thousand airline reservation stations are computing for the use of a single slotted ALOHA channel. The average station makes 18 request/hour. A slot is 125 μ sec. What is the approximate total channel load ? (See Unit-III, Page 118, Prob.2) 10

Unit-IV

7. (a) Differentiate between adaptive routing and non adaptive routing. (See Unit-IV, Page 146, Q.8) 10

(b) How congestion effects the communication subnet ? Explain any 2 strategies for controlling congestion. ** 10

Or

8. (a) What is internetworking ? Describe in brief the working of concatenated virtual circuitry way of internetworking. ** 10

(b) Explain the packet discarding approach of flow control. 10

Unit-V

9. (a) What are the services provided by transport layer ? (See Unit-I, Page 32, Q.30) 10

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Msinventer

(b) What is network security and write the aspects of network security ? ** 10

Or

10. Write short notes on (any two) – 20

(a) Bluetooth (See Unit-III, Page 139, Q.55)

(b) Mobile IP **

(c) Cryptography **

(d) DNS. (See Unit-V, Page 220, Q.43)

RGPV

B.E. (Sixth Semester) EXAMINATION, June 2014
(Computer Science Engg. Branch)
COMPUTER NETWORKING
(CS-604)

Note : 1. There are five units.
2. Attempt one question from each unit.
3. All questions carry equal marks

Unit-I

1. (a) Explain the ISO-OSI model of computer network. Give the function of each layer. (See Unit-I, Page 27, Q.27) 7

(b) Explain queueing system. Discuss Little's theorem. ** 7

Or

2. (a) Explain TCP/IP model in brief. Differentiate it with seven layered model. (See Unit-I, Page 36, Q.37) 7

(b) Explain the working of –

(i) Connection oriented and

(ii) Connectionless services. What are their advantages, disadvantages and appplications ? (See Unit-I, Page 21, Q.21) 7

Unit-II

3. (a) Name important functions of data link layer. Explain flow control and error control. (See Unit-II, Page 63, Q.11) 7

(b) Explain stop and wait protocol. Derive the expression for utilization. (See Unit-II, Page 67, Q.19) 7

Or

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

4. (a) Explain sliding window protocol. Also explain how does it help to reduce congestion. (See Unit-II, Page 71, Q.23) 7

(b) What is piggybacking ? (See Unit-II, Page 64, Q.14)
write a note on HDLC. ** 7

Unit-III

5. (a) Explain the terms 'Static channel allocation' and 'dynamic channel allocation'. (See Unit-III, Page 100, Q.6) 7

(b) Write a short note on ALOHA. Differentiate Pure ALOHA and slotted ALOHA. (See Unit-III, Page 106, Q.14) 7

Or

6. (a) Compare collision, collision free and limited contention MAC sub layer protocol with suitable examples. (See Unit-III, Page 126, Q.38) 7

(b) What are the different line coding techniques ? Which is used in 802.3 LAN ? (See Unit-III, Page 131, Q.45) 7

Unit-IV

7. (a) Differentiate logical, classful and classless addressing techniques. 7
(See Unit-IV, Page 170, Q.33)

(b) With the help of suitable diagrams explain unicast, multicast and broadcast routing. (See Unit-IV, Page 161, Q.23) 7

Or

8. (a) Give a comparative study of IPv4 and IPv6. 7
(See Unit-IV, Page 181, Q.47)

(b) What is congestion control ? Explain the leaky bucket mechanism for congestion control. ** 7

Unit-V

9. Write short note on any four of the followings – 14

(i) UDP Header format (See Unit-V, Page 187, Q.9)

(ii) TCP Header format (See Unit-V, Page 201, Q.24)

(iii) HTTP (See Unit-V, Page 208, Q.30)

(iv) Network Management (See Unit-V, Page 222, Q.46)

(v) Presentation layer protocol (any one) **

(vi) DNS. (See Unit-V, Page 220, Q.43)

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Msinverter

RGPV

B.E. (Sixth Semester) EXAMINATION, Dec. 2014
(Computer Science Engg. Branch)
COMPUTER NETWORKING
(CS-604)

Note : Total number of questions 10. Attempt one question (including all parts) from each unit. Assume missing data, if any, suitably.

1. **(a)** Explain how message exchange takes place between machine A and B using TCP connection. (See Unit-V, Page 189, Q.12)

   (b) How does the layer of TCP/IP protocol suite correlate to the layers of OSI model ? (See Unit-I, Page 34, Q.34)

2. How does Frame relay differ from ATM ? **

3. **(a)** Explain the Noisy Channel Protocol; Go-Back-N ARQ. (See Unit-II, Page 76, Q.27)

   (b) What are the various connecting devices used in networking ? Explain design and functioning of Bridges. **

4. **(a)** Using CRC a bit stream 1101011011 is to be transmitted. If the generator polynomial is find the

   (b) Compare the performance of stop and wait protocol and sliding window protocol. (See Unit-II, Page 84, Q.32)

5. **(a)** Explain ALOHA and slotted ALOHA protocol. Compare the efficiency in each case. (See Unit-III, Page 107, Q.16)

   (b) Compare IEEE 802.3, 802.4 and 802.5. (See Unit-III, Page 136, Q.53)

   Or

6. **(a)** Explain why token bus is suited for real time application in comparison to CSMA/CD with the help of suitable examples. (See Unit-III, Page 136, Q.52)

   (b) Suppose a group of N stations share a 56 kbps pure ALOHA channel. Each station outputs 1000 bit frame on an average of once every 100 sec even if the previous one has not yet been sent (e.g. the stations can buffer outgoing frames). What is the maximum value of N ? (See Unit-III, Page 117, Prob.1)

7. **(a)** What is congestion control and how it is implemented in network layer ? What is the role of Choke packet in managing congestion ? **

   (b) What is the isolated routing ? Explain one isolated routing in details. (See Unit-IV, Page 162, Q.25)

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

8. **(a)** Explain IPv4 header format with the help of a neat diagram. State four major improvements of IPv6 over IPv4. (See Unit-IV, Page 178, Q.44)

   (b) Describe a way to do reassembly of IP fragments at the destination. (See Unit-IV, Page 144, Q.3)

9. **(a)** Explain the working of User Datagram Protocol. (See Unit-V, Page 184, Q.4)

   (b) What is Cryptography ? Explain Public and Private Keys to be used for Cryptography mechanism. **

   Or

10. **(a)** Explain the working of TCP protocol and how the connection is released in a TCP. (See Unit-V, Page 193, Q.18)

    (b) Explain the functioning and steps used in Substitution and transposition ciphers. **

RGPV

B.E. (Sixth Semester) EXAMINATION, June 2015
(Computer Science Engg. Branch)
COMPUTER NETWORKING
(CS-604)

Note : **(i)** Answer five questions. In each question part A, B, C is compulsory and D part has internal choice.

(ii) All parts of each questions are to be attempted at one place.

(iii) All questions carry equal marks, out of which part A and B (Max. 50 words) carry 2 marks, part C (Max. 100 words) carry 3 marks, part D (Max. 400 words) carry 7 marks.

(iv) Except numericals, Derivation, Design and Drawing etc.

Unit-I

1. **(a)** What is multicasting ? (See Unit-I, Page 13, Q.10)

   (b) Write any two differences between connection oriented and connection less services. (See Unit-I, Page 21, Q.21) **

   (c) What is Little's formula ? Prove it.

   (d) During the communication, how various layers of OSI model exchange information to establish a connection ? Describe with the help of a suitable diagram. (See Unit-I, Page 27, Q.27)

   Or

   Discuss Markov chain model and Explain M/G/1 queues. **

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Unit-II

2. **(a)** What are the various functions performed by the data link layer ? **(See Unit-I, Page 32, Q.29)**

(b) What do mean by protocol verification ? **(See Unit-II, Page 87, Q.34)**

(c) Explain the mechanism of stop and wait ARQ. **(See Unit-II, Page 76, Q.28)**

(d) Explain the following protocols –

(i) SDLC

(ii) LAP and LAPB. **

Or **

A channel of one Mbps with propagation delay of 270 ms transmits frames of size 1000 bits. What is the maximum link utilization for stop-and-wait, and sliding window with window size 7 ? **(See Unit-II, Page 85, Prob.2)**

Unit-III

3. **(a)** Differentiate between 1-persistent CSMA and p-persistent CSMA protocols. **(See Unit-III, Page 111, Q.22)**

(b) What is channelization ? Define time Division Multiple Access. **(See Unit-III, Page 111, Q.23)**

(c) Explain URN protocol. **(See Unit-III, Page 127, Q.40)**

(d) Explain the following –

(i) High speed LAN (ii) Fast Ethernet (iii) FDDI. **

Or

Define the throughput of Pure ALOHA ? A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kpbs. What is the throughput if the system (all stations together) produces –

(i) 1000 frames per second (ii) 500 frames per second

(iii) 250 frames per second. **(See Unit-III, Page 119, Prob.5)**

Unit-IV

4. **(a)** What is IPv4 Protocol ? **(See Unit-IV, Page 176, Q.40)** **

(b) What is Mobile IP ?

(c) What is IP Addresses ? Categorize the IP addresses into various classes. **(See Unit-IV, Page 165, Q.27)**

(d) How does link state routing take care of the problem of wrapping of sequence numbers, crashing of routers and corruption of sequence number ? **(See Unit-IV, Page 148, Q.11)**

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Or

What is Dijkstra algorithm ? Using Dijkstra algorithm find the shortest path from 0 to 4.

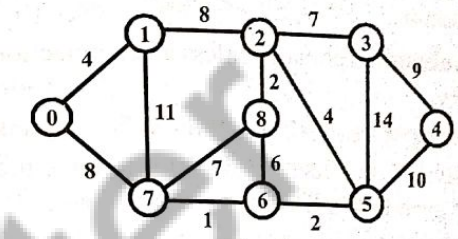


Fig. 1

(See Unit-IV, Page 163, Prob.1)

Unit-V

5. **(a)** What is the utility of DNS ? **(See Unit-V, Page 220, Q.43)**

(b) What are the various transmission modes of FTP ? **(See Unit-V, Page 212, Q.35)**

(c) What is World Wide Web ? Explain the architecture of www. **(See Unit-V, Page 205, Q.29)**

(d) Briefly explain two protocols used in Transport Layer for Internet. Explain the TCP service model and segment header. **(See Unit-V, Page 202, Q.25)**

Or

How Connection is established and Terminated in TCP using Three way handshaking mechanism ? Describe in detail. **(See Unit-V, Page 192, Q.17)**

RGPV

B.E. (Sixth Semester) EXAMINATION, Dec. 2015
(Computer Science Engg. Branch)
COMPUTER NETWORKING
(CS-604)

Note : (i) Answer five questions. In each question part A, B, C is compulsory and D part has internal choice.

(ii) All parts of each questions are to be attempted at one place.

(iii) All questions carry equal marks, out of which part A and B (Max. 50 words) carry 2 marks, part C (Max. 100 words) carry 3 marks, part D (Max. 400 words) carry 7 marks.

(iv) Except numericals, Derivation, Design and Drawing etc.

MSinventer

Unit-I

(a) What are two reasons for using layered protocols ? What is one possible disadvantage of using layered protocols ?

(See Unit-I, Page 19, Q.17)

(b) Differentiate between connectionless and connection-oriented services of networks.

(See Unit-I, Page 21, Q.21)

(c) Define queuing system. Also explain M/M/1 Queue model. **

(d) Draw the layered architecture of OSI reference model. Also explain function of each in brief.

(See Unit-I, Page 27, Q.27)

Or

Explain the term services, interfaces and protocol in details. Give the relationships between services and protocols.

(See Unit-I, Page 20, Q.20)

Unit-II

(a) A bit string, 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing?

(See Unit-II, Page 61, Q.7)

(b) Give at least one reason why PPP uses byte stuffing instead of bit stuffing to prevent accidental flag bytes within the payload from causing confusion. **

(c) Describe various error detecting protocols use at data link layer. **

(d) Discuss the difference between bit oriented and byte oriented protocol. Also explain various frames use in HDLC protocol. **

Or

What is an ARQ ? Explain different ARQ techniques.

(See Unit-II, Page 74, Q.26)

Unit-III

(a) Sketch the Manchester encoding on a classic ethernet for the bit stream 0001110101.

(See Unit-III, Page 121, Prob.7)

(b) A group of N stations share a 56-kbps pure ALOHA channel. Each station outputs a 1000-bit frame on average once every 100 sec, even if the previous one has not yet been set (e.g., the stations can buffer outgoing frames). What is the maximum value of N ?

(See Unit-III, Page 117, Prob.1)

(c) How does CSMA/CD protocol improve the performance over CSMA protocol for long frames ?

(See Unit-III, Page 113, Q.27)

*Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

(d) Compare collision, collision free and limited contention MAC layer protocols with suitable example.

(See Unit-III, Page 126, Q.38)

Or

Describe the frame format of IEEE 802.3 standard for MAC sublayer.

(See Unit-III, Page 132, Q.46)

Unit-IV

(a) Datagram networks route each packet as a separate unit, independent of all others. Virtual-circuit networks do not have to do this, since each data packet follows a predetermined route. Does this observation mean that virtual-circuit networks do not need the capability to route isolated packets from an arbitrary source to an arbitrary destination? Explain your answer.

(See Unit-IV, Page 143, Q.2)

(b) A computer on a 6-Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 1 Mbps. It is initially filled to capacity with 8 megabits. How long can the computer transmit at the full 6-Mbps ? **

(c) Justify the need of logical addressing scheme in networking. Also explain how a physical address is mapped into a logical address.

(See Unit-IV, Page 170, Q.34)

(d) A host in an organization has an IP address 150.37.64.34 and a subnet mask 255.255.240.0. Find the followings –

(i) What is the address of this subnet ?

(ii) What are the ranges of IP address that is host can have on this subnet ?

(See Unit-IV, Page 182, Prob.3)

Or

What is routing ?

(See Unit-IV, Page 145, Q.5)

Explain different parameters on which the dynamic routing algorithms can be designed. Also contrast one with another.

Unit-V

(a) Describe working of SMTP protocol in brief.

(See Unit-V, Page 216, Q.39)

(b) Both UDP and TCP use port numbers to identify the destination entity when delivering a message. Give two reasons why these protocols invented a new abstract ID (port numbers), instead of using process IDs, which already existed when these protocols were designed.

(c) Explain the header format of UDP protocol.

(See Unit-V, Page 187, Q.9)

*Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

MSIRVE

(d) With neat diagram explain the process of connection establishment and release using 3-way handshaking in transport layer.

(See Unit-V, Page 192, Q.17)

Or

What are the functions of presentation layer ? Justify the necessity of presentation layer in the architecture of OSI with suitable example.

(See Unit-I, Page 32, Q.31)

RGPV

B.E. (Sixth Semester) EXAMINATION, June 2016
(Computer Science Engg. Branch)
COMPUTER NETWORKING
(CS-604)

ote : (i) Answer five questions. In each question part A, B, C is compulsory and D part has internal choice.

(ii) All parts of each questions are to be attempted at one place.

(iii) All questions carry equal marks, out of which part A and B (Max. 50 words) carry 2 marks, part C (Max. 100 words) carry 3 marks, part D (Max. 400 words) carry 7 marks.

(iv) Except numericals, Derivation, Design and Drawing etc.

Unit-I

. (a) What are the uses of computer network now-a-day ?

(See Unit-I, Page 6, Q.4)

(b) What is the difference between TCP and UDP ?

(See Unit-V, Page 190, Q.13)

(c) What is the principle difference between connectionless communication and connection-oriented communication ?

(See Unit-I, Page 21, Q.21)

(d) Explain the layered architecture of OSI model. List two ways in which OSI model and TCP/IP model are same.

(See Unit-I, Page 36, Q.35)

Or

What are the types of queuing system is used for computer network ? Explain. **

Unit-II

2. (a) How framing is done in data link layer ? Explain.

(See Unit-II, Page 57, Q.3)

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

(b) What is the role of bit stuffing in data transmission ?

(See Unit-II, Page 60, Q.5)

(c) What is remainder obtained by dividing $x^7 + x^5 + 1$ by the generator polynomial $x^3 + 1$?

(See Unit-II, Page 86, Prob.4)

(d) What conditions would have to hold for a corrupted frame to circulate forever on a token ring without a monitor ? How does the monitor fix this problem ?

(See Unit-III, Page 136, Q.51)

Or

Data link protocols almost always put the CRC in a trailer rather than in header. Why ?

(See Unit-II, Page 64, Q.13)

Unit-III

3. (a) How is possible to allocate static channel in LANs and MANs ?

(See Unit-III, Page 102, Q.7)

(b) How adaptive tree walk protocol works ? (See Unit-III, Page 126, Q.36)

(c) What is the difference between Multiple Access and Collision Avoidance (MACA) and MACAW (for wireless) ?

(See Unit-III, Page 126, Q.39)

(d) Consider the delay of pure ALOHA versus slotted ALOHA at the low load. Which one is less ? Explain your answer.

(See Unit-III, Page 105, Q.11)

Or

Store-and-forward switches have an advantage over cut-through switches with respect to damaged frames. Explain what it is. **

Unit-IV

4. (a) Explain the store-and-forward packet switching. **

(b) How datagram subnet is differ from virtual-circuit subnet ? **

(c) How count-to-infinity problem is generated in routing algorithm ?

(See Unit-IV, Page 154, Q.15)

(d) How Open Shortest Path First (OSPF) work ? Explain with an example.

(See Unit-IV, Page 155, Q.17)

Or

What is resource reservation protocol and how is it work ? **

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Mahveer

Unit-V

(a) The maximum payload of a TCP segment is 65,515 bytes. Why was such a strange number chosen ? (See Unit-IV, Page 191, Q.15)

(b) Give the advantages of RPC on UDP over transactional TCP. (See Unit-V, Page 192, Q.16)

(c) What is the role of SMTP and POP 3 in a mail services ? (See Unit-V, Page 217, Q.40)

(d) DNS uses UDP instead of TCP. If a DNS packet is lost, there is no automatic recovery. Does this cause a problem ? And if so, how is it solved ? (See Unit-V, Page 221, Q.44)

Or

Write short notes on –

(i) SSH

(ii) LPP (See Unit-V, Page 213, Q.36)

(iii) Telnet. **

**

RGPV

B.E. (Sixth Semester) EXAMINATION, Dec. 2016
COMPUTER NETWORKING
(CS-604)

te : (i) Answer five questions. In each question part A, B, C is compulsory and D part has internal choice.

(ii) All parts of each questions are to be attempted at one place.

(iii) All questions carry equal marks, out of which part A and B (Max. 50 words) carry 2 marks, part C (Max. 100 words) carry 3 marks, part D (Max. 400 words) carry 7 marks.

(iv) Except numericals, Derivation, Design and Drawing etc.

(v) Assume suitable value for missing data, if any.

(a) What is Protocol ? (See Unit-I, Page 17, Q.14)

(b) Why star topology is commonly preferred ? (See Unit-I, Page 11, Q.7)

(c) What is the difference between connectionless communication and connection oriented communication ? (See Unit-I, Page 21, Q.21)

(d) Discuss the M/M/1 queueing system with infinity capacity and obtain its steady state probability and mean no. of customer in the system. **

Or

Compare OSI and TCP/IP reference model. (See Unit-I, Page 34, Q.34)

*Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

2. (a) Define Data transparency. (See Unit-II, Page 61, Q.8)

(b) Define Error control. (See Unit-II, Page 63, Q.10)

(c) What are the reasons for breaking a long data transmission up into a number of frames ? (See Unit-II, Page 67, Q.16)

(d) Two stations communicate via a 1 Mbps satellite link with a propagation dealy of 270 ms. The satellite serves merely to retransmit data received from one station to another, with negligible switching delay. Using HDLC frames of 1024 bits with 3-bit sequence numbers, what is the maximum possible data throughput ? **

Or

Compare the performance of stop and wait protocol and sliding window protocol.

3. (a) What is random access ? (See Unit-II, Page 84, Q.32)

(b) How can you compare 1-persistent CSMA and P-Persistent CSMA ? (See Unit-III, Page 98, Q.3)

(c) Fast Ethernet has the same 64 byte minimum frame size but can get bits out ten times faster. How is it possible to maintain the same frame size ? How much bandwidth loss will occur in this case ? (See Unit-III, Page 111, Q.22) **

(d) Differentiate between 802.3, 802.4 and 802.5 IEEE standard. (See Unit-III, Page 136, Q.53)

Or

Evaluate the ring latency of 20 stations separated by 100 metres and operate at a speed of 4 Mbps. Assume the delay introduced by each station to be 2.5 bit. (See Unit-III, Page 142, Prob.3)

4. (a) What do you mean by Unicast Routing ? (See Unit-IV, Page 161, Q.22)

(b) What is the difference between congestion control and flow control ? **

(c) Write the desired property of routing algorithm. (See Unit-IV, Page 145, Q.7)

(d) Describe multicasting in the mobile IP protocol. Show, using diagram, the difference between the bidirectional tunnel multicast method and the remote subscription multicast method.

Or

Apply Dijkstra's routing algorithm to calculate shortest path with source vertex 'A'.

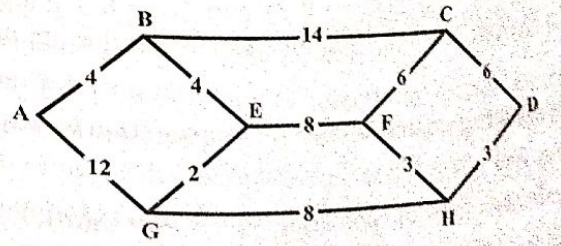


Fig. 1

(See Unit-IV, Page 164, Prob.2)

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

(a) What is Data compression ?

(b) Explain flow control in TCP. ** (See Unit-V, Page 196, Q.22)

(c) In cases where reliability is not a primary importance, UDP would make a good transport protocol. Give examples of specific cases. (See Unit-V, Page 185, Q.5)

(d) Explain SMTP protocol in detail. (See Unit-V, Page 216, Q.39)

Or

What is FTP ? How FTP differs from other internet applications and also gives the important features of FTP ? (See Unit-V, Page 212, Q.34)

RGPV

B.E. (Sixth Semester) EXAMINATION, June 2017
COMPUTER NETWORKING
(CS-604)

te : (i) Answer any five questions.

(ii) All questions carry equal marks.

Explain the X.25 packet formats with suitable diagrams. **

What do you mean by broadcast network ? Discuss the need or lack of need for a network layer in a broadcast network. (See Unit-I, Page 13, Q.11)

Explain IEEE 802.2 in detail. (See Unit-III, Page 129, Q.43)

Explain serial line IP and point to point protocol. **

What do you mean by medium Access control sublayer ? Why do we need it ? Explain MAC. (See Unit-III, Page 97, Q.1)

Consider a slotted ALOHA having five stations. If the offered load G_1 = 0.1, G_2 = 0.15, G_3 = 0.2, G_4 = 0.25 and G_5 = 0.3 packets, find the individual throughput of each station and channel throughput. (See Unit-III, Page 120, Prob.6)

Explain multicasting routing in brief. (See Unit-IV, Page 161, Q.20)

Answer any four of the following –

(a) Write the functions of each layer. (See Unit-I, Page 32, Q.28) **

(b) Name the types of HDLC frames.

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

(c) How does CSMA/CD protocol improve the performance over CSMA protocol for long frames ? (See Unit-III, Page 113, Q.27)

(d) Explain the frame format of IPv4. (See Unit-IV, Page 177, Q.42)

(e) Give the format of UDP datagram. (See Unit-V, Page 187, Q.9)

(f) How does TCP achieve reliability in data transmission ? (See Unit-V, Page 196, Q.21)

RGPV

CS-604 (GS)
B.E. (Sixth Semester) EXAMINATION, Dec. 2017
Grading System (GS)
COMPUTER NETWORKING

Note : (i) Answer any *five* questions.

(ii) All questions carry equal marks.

1. Explain the design issues and functionality of ISO-OSI model. (See Unit-I, Page 33, Q.32)

2. Differentiate between connectionless and connection-oriented services. Discuss their advantages, disadvantages and typical applications. (See Unit-I, Page 21, Q.21)

3. Discuss and compare DLL "Go Back n" and "Selective repeat" protocols. (See Unit-II, Page 77, Q.29)

4. Draw the frame format of HDLC protocol. Explain the technique of bit stuffing for data transparency. Explain the use of control, data checksum and address field of HDLC. **

5. Derive an expression to prove that throughput of "Slotted ALOHA" is approximately twice and than that of "PURE ALOHA". (See Unit-III, Page 107, Q.17)

6. What are the tasks of FDDI medium access control protocol ? What type of traffic is handled by a FDDI networks ? **

7. Explain the Bellman-Ford routing algorithm. Discuss the drawback of count to infinity in Bellman-Ford algorithm. (See Unit-IV, Page 155, Q.16)

8. Answer any four of the following –

(a) Explain interfaces and services. (See Unit-I, Page 20, Q.19)

(b) How does sliding window protocol help to reduce congestion to an extent ? (See Unit-II, Page 71, Q.22)

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

MSinventer

(c) What is the effect of delay time in ALOHA on its throughput ? (See Unit-III, Page 105, Q.12)

(d) What is congestion control ? Write general principles of congestion control. **

(e) Why is UDP needed ? Why can't user program directly access IP ? (See Unit-V, Page 187, Q.8)

(f) Differentiate between TCP and UDP. (See Unit-V, Page 190, Q.13)

RGPV

CS-6004 (CBGS)
B.E. (Sixth Semester) EXAMINATION, May 2018
Choice Based Grading System (CBGS)
COMPUTER NETWORKING

Note : (i) Attempt any *five* questions.
(ii) All questions carry equal marks.
(iii) Assume suitable data if missing.

1. (a) Explain the principles that were applied at the time of seven layer architecture design of ISO-OSI reference model. 7 (See Unit-I, Page 27, Q.26)

(b) What is queuing theory ? Explain the queuing system M/M/1. 7 **

2. (a) Two networks each provide reliable byte connection oriented service. One of them offers a reliable byte stream and the other offers a reliable message stream. Are these identical ? If so, why is distinction made ? If not, given an example of how they are differ ? 7 (See Unit-I, Page 23, Q.22)

(b) Write the goals of computer networking with its classification. 7 (See Unit-I, Page 4, Q.3) ** 7

3. (a) Compare and contrast SDLC with HDLC.

(b) What is the mechanism of sliding window flow control ? Explain with example. (See Unit-II, Page 68, Q.20) 7

4. (a) If the start and end header is 100001 and the following data stream is to be stuffed –
100110001100001110000011
What will be the frame after bit stuffing ? 7

(b) Write the different types of ARQ techniques. (See Unit-II, Page 74, Q.26)

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

5. (a) What are the performance measuring metric for a computer network ? Define each of them. (See Unit-III, Page 128, Q.41) 7

(b) A large population of ALOHA users manage to generate 50 request/sec including both originals and retransmissions. Time is slotted in units of 40 msec. 7
(i) What is the chance of success in the first attempt ?
(ii) What is the probability of exactly k collisions and then success ? (See Unit-III, Page 119, Prob.4)

6. (a) Make a comparison between pure ALOHA, slotted ALOHA and CSMA/CD. (See Unit-III, Page 112, Q.25) 7

(b) Explain the frame format of IEEE 802.4 (token bus) protocol. 7 (See Unit-III, Page 135, Q.50)

7. (a) Describe the working of Bellman ford algorithm using suitable example. (See Unit-IV, Page 152, Q.14) 7

(b) Write the general principles of congestion control. ** 7

8. Write short notes on – 14
(i) HTTP (See Unit-V, Page 208, Q.30)
(ii) Packet format of UDP (See Unit-V, Page 187, Q.9)
(iii) SMTP. (See Unit-V, Page 216, Q.39)

RGPV

CS-6004 (CBGS)
B.E. VI Semester
EXAMINATION, May 2019
Choice Based Grading System (CBGS)
COMPUTER NETWORKING

Note : (i) Attempt any five questions.
(ii) All questions carry equal marks.

1. (a) Explain network architecture in detail. (See Unit-I, Page 12, Q.9) 7

(b) State the major funtions performed by the presentation layer of the ISO-OSI model. (See Unit-I, Page 32, Q.31) 7

2. (a) Explain TCP connection management. (See Unit-V, Page 186, Q.30) 7

(b) Explain different flow control mechanisms used in brief. 7 (See Unit-II, Page 71, Q.21)

3. (a) What is framing ? Explain different types of framing protocols with their format. (See Unit-II, Page 60, Q.4) 7

(b) Explain different error detection and correction mechanisms with examples. ** 7

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

MU Venter

4. (a) Explain CSMA and protocols with collision detection and avoidance. 7
(See Unit-III, Page 115, Q.30)

(b) What is internetworking ? Explain its service model, global address and packet format. ** 7

5. (a) Explain the functioning of wireless LAN in detail. 7
(See Unit-III, Page 138, Q.54)

(b) Explain the salient features of IPv6. (See Unit-IV, Page 179, Q.45) 7

6. (a) Explain Bellman-Ford algorithm with example. 7
(See Unit-IV, Page 152, Q.14)

(b) What do you mean by routing ? Explain Hierarchical, Broadcast and Multicast routing. (See Unit-IV, Page 161, Q.21) 7

7. (a) Explain transport layer multiplexing and demultipexing. 7
(See Unit-V, Page 203, Q.27)

(b) Write the HTTP request and HTTP response message format. 7
(See Unit-V, Page 208, Q.31)

8. (a) Explain the services provided by DNS. (See Unit-V, Page 222, Q.45) 7

(b) Enlist the protocols of presentation layer. Explain the working of any one protocol. ** 7

❑❑❑

**Now, according to new revised syllabus of R.G.P.V., it is not included in syllabus

Msinventer